PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/08 | A1

(11) International Publication Number: WO 95/17059

(43) International Publication Date: 22 June 1995 (22.06.95)

(21) International Application Number: PCT/US94/14309

(22) International Filing Date: 14 December 1994 (14.12.94)

(30) Priority Data:
08/167,678 15 December 1993 (15.12.93) US
08/183,602 18 January 1994 (18.01.94) US

(71)(72) Applicants and Inventors: MANKOVITZ, Roy, J. [US/US]; 18057 Medley Drive, Encino, CA 91316 (US). NG, Yee, Kong [GB/GB]; 18 H Block 4, Uptown Plaza, Tai Po, N.T. (HK).

(74) Agent: HARTZ, Edwin, L.; Christie, Parker & Hale, P.O. Box 7068, Pasadena, CA 91109-7068 (US).

(81) Designated States: AM, AT, AU, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, JP, KE, KG, KP, KR, KZ, LK, LR, LT, LU, LV, MD, MG, MN, MW, NL, NO, NZ, PL, PT, RO, RU, SD, SE, SI, SK, TJ, TT, UA, UZ, VN, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), ARIPO patent (KE, MW, SD, SZ).

Published

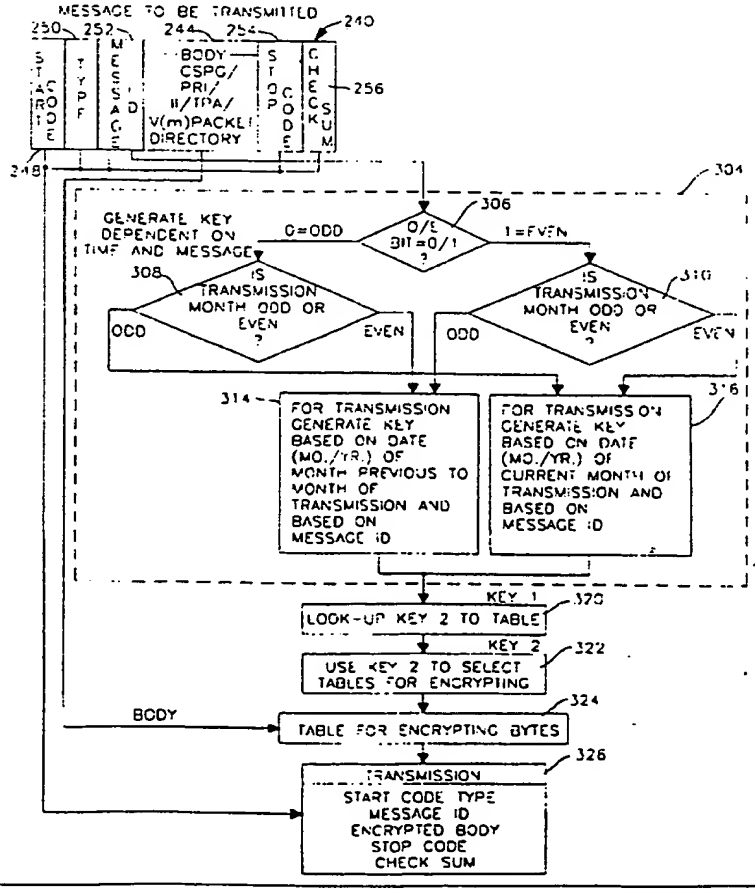
With international search report.

Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: METHOD FOR ENCRYPTING AND EMBEDDING INFORMATION IN A VIDEO PROGRAM

(57) Abstract

A method is provided for transmitting information having a header portion (242) and a body portion (244), the method includes the steps of providing a clock (80), generating (316) a first key base on the clock (80) and a part of the header portion (242), using the first key for encrypting the body portion (244) to generate an encrypted body portion, combining the encrypted body portion and the header portion to form a data packet (240), combining a video program and the data packet (240) to form and transmit a composite video signal (326). After encryption the encrypted body portion can be scrambled by using a scrambling key to swap the bits of the body portion. A method for receiving transmitted information having a header portion (242) and an encrypted body portion comprises the steps of providing a clock (80), generating (318) a first key based on the clock (80) and a part of the header portion (242), using the first key for decrypting the encrypted body portion to generate a decrypted body portion, combining the decrypted body portion and the header portion to form a data packet, and recording the data packet on a video cassette tape (328).



3DOCID: <WO__9517059A1_I_>

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria
AU	Australia
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CS	Czechoslovakia
CZ	Czech Republic
DE	Germany
DK	Denmark
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgystan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakhstan
LI	Liechtenstein
LK	Sri Lanka
LU	Luxembourg
LV	Larvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SI	Slovenia
SK	Slovakia
SN	Senegal
TD	Chad
TG	Togo
TJ	Tajikistan
TT	Trinidad and Tobago
UA	Ukraine
US	United States of America
UZ	Uzbekistan
VN	Viet Nam

METHOD FOR ENCRYPTING AND EMBEDDING INFORMATION IN A VIDEO PROGRAM

This is application is based on priority of pending U.S. Patent application Serial No. 08/167,678 filed December 15, 1993, and U.S. Patent application 08/183,602, filed January 18, 1994 both of which are incorporated herein by this reference as though set forth in full.

Background of the Invention

Field of the Invention:

This invention relates generally to methods for scrambling and encrypting information embedded in a video program that is transmitted over the air, cable, satellite or telephone lines, or that is recorded on a video cassette tape.

Description of the Related Art:

Television programs can include closed captioning and other information embedded in the program. This information can be embedded in the vertical blanking interval (VBI) lines (described below) of a television video signal. A VBI decoder in a VCR or a television is used to retrieve the closed captions, which are for the hearing impaired, and other information from the VBI lines. The closed captions are then displayed as text on the television monitor along with the video.

Other information can also be embedded in the VBI lines. For example, a directory to programs can be embedded in the VBI lines. The directory can either be transmitted in the VBI lines during a transmission over the air, cable, satellite or telephone lines or stored in the VBI lines of a video cassette tape along with the programs on the video cassette tape. The directory can then be used to control a video cassette recorder (VCR) to access programs on the video cassette tape. Other information in the VBI lines can include channel specific program guide (CSPG), program related information (PRI), Instant Information (II), video magazine (V(M)) packet, and tape identification, program number and absolute address (TPA) packet, which are described below.

Since the information provides valuable services for users, it is necessary to control access to the information to only authorized users. Otherwise revenue for the services cannot be collected.

Summary of the Invention

An object of the present invention is provide methods and apparatus for scrambling and encrypting information embedded in a video program that is either transmitted or that is recorded on a video cassette tape.

Another object of the present invention is to provide methods for descrambling and

DOCID: <WO__9517068A1_I_>

Accordingly apparatus and methods for scrambling and encrypting and descrambling and decrypting are provided. In one embodiment of the present invention a method for transmitting information having a header portion and a body portion includes the steps of providing a clock having an output as a function of time, generating a first key based on the time from the clock and a part of the header portion, using the first key for encrypting the body portion to generate an encrypted body portion, combining the encrypted body portion and the header portion to form a data packet, combining a video program and the data packet to form a composite video signal, and transmitting the composite video signal.

In another embodiment of the present invention a method for receiving transmitted information having a header portion and an encrypted body portion includes the steps of providing a clock having an output as a function of the time, generating a first key based on the time from the clock and a part of the header portion, using the first key for decrypting the encrypted body portion to generate a decrypted body portion, combining the decrypted body portion and the header portion to form a data packet, and recording the data packet on a video cassette tape.

In another embodiment of the present invention a method for recording information having a body portion and a header portion on a video cassette tape includes the steps of providing a clock having an output as a function of the time, generating a first key based on the time from the clock and a part of the header portion, using the first key for encrypting the body portion to generate an encrypted body portion, embedding the encrypted body portion and the header portion within the video program, and recording the video signal on a video cassette tape.

In another embodiment of the present invention a method for decrypting recorded information having a header portion and an encrypted body portion, includes the steps of providing a clock having an output as a function of the time, generating a first key based on the time from the clock and a part of the header portion, and using the first key for decrypting the encrypted body portion to generate a decrypted body portion.

Other objects and many of the attendant features of this invention will be more readily appreciated as the same becomes better understood by reference to the following detailed descriptions and considered in connection with the accompanying drawings in which like reference symbols designate like parts throughout the figures.

Brief Description of the Drawings

FIG. 1A is a block diagram illustrating an indexing video cassette recorder that operates with a directory controller to provide access to indexed programs recorded on a video cassette tape in accordance with principles of the invention.

FIG. 1B is a block diagram of a transmitter in accordance with principles of the invention.

FIG. 2 is a diagram illustrating the fields, frames and vertical blanking interval of an interlaced television scanning raster.

FIG. 3 is a diagram illustrating the timing of the vertical blanking interval (VBI) lines of an interlaced television scanning raster and the information that can be embedded in the VBI lines.

FIG. 4 is a schematic view of an embodiment for recorded tapes illustrating storing VISS marks on a control track, TPA packets each containing a tape identification number, a program number, and an absolute address in a vertical blanking interval line, and a directory in a vertical blanking interval line in accordance with principles of the invention.

FIG. 5A is a schematic conceptually illustrating the information in a TPA packet in accordance with principles of the invention.

FIG. 5B is a schematic conceptually illustrating the information in a directory for a program in accordance with principles of the invention.

FIG. 6 is a schematic conceptually illustrating the header, body and end of a CSPG, PRI, Instant Information (II), V(M) packet, or directory as stored in a VBI line in accordance with principles of the invention.

FIG. 7 is a illustration of the relationship of the Odd/Even bit to the months of a year according to the present invention.

FIG. 8A is a flow chart of a method for encrypting information embedded in a video program that is transmitted according to the present invention.

FIG. 8B is a flow chart of a method for encrypting information embedded in a video program that is recorded on a video cassette tape according to the present invention.

FIG. 9A is a flow chart of a method for decrypting information embedded in a video program that is transmitted according to the present invention.

FIG. 9B is a flow chart of a method for decrypting information embedded in a video program that is recorded on a video cassette tape according to the present invention.

FIG. 10 is an illustration of the method of mapping bytes of a body to encrypted bytes according to the present invention.

FIG. 11 is an illustration of the method of mapping encrypted bytes of a body to decrypted bytes according to the present invention.

OCID: <WO__9517059A1_1_>

Detailed Description

Referring to the drawings, FIG. 1A is a block diagram of an indexing VCR system 10 including a video cassette recorder (VCR) 1 with a video tape cassette 40, a video display 50, and a directory controller 30. The VCR 1 is a conventional video cassette recorder device and uses any one of many different recording technologies such as BETA, VHS, super VHS, 8 mm, VHS-C or any other popular technology. Particularly useful are VHS-C indexed tapes, which can be played directly on a VHS indexing VCR that has a full index function as described in U.S. application Ser. No. 08/066,666. The cassette 40 is a conventional video cassette having a magnetic tape 42 packaged in a cartridge or cassette housing. Even though the size and design of the housing is different for different types of recording technology, the basic information that goes on the tape itself is similar. The technology and operation of a VCR are well understood in the art.

The VCR 1 has a button control panel 3 with control buttons, including LOAD 3a, PLAY 3b, STOP 3c, RECORD 3d, and EJECT 3e, for controlling the operation of the VCR 1. The LOAD button 3a is optional and is not used on machines which load automatically. The VCR control logic circuit 21 receives control signals from the button control panel 3 and controls the overall operation of the VCR 1 by sending control signals to motor control 5, a video logic circuit 7, and a position logic and counter circuit 9, as well as, to video display 50 and microprocessor controller 31 of the directory controller 30. A clock 80 can be set to a time and read by the VCR control logic. The VCR control logic 21 can be implemented with a microprocessor and a memory for storing programs to implement the steps of the methods of the invention.

The motor control 5 controls loading and ejecting of the cassette 40 and also controls movement of the video tape 42 within the video cassette 40 during record, play, search, fast forward, and rewind operations. The video logic circuit 7 controls the operation of video read/write head 14 in reading from or recording video signals to the tape 42. As a program is recorded and played, the tape 42 is passed around capstan 13. The speed of capstan 13 is controlled by motor control 5 to maintain a constant linear tape speed during record, play and search operations. Search speed is about twice as fast as play speed. In rewind and fast forward operations the tape speed is controlled by the speed of the supply or take-up reels. The position logic and counter circuit 9 monitors tape movement through a cassette tape movement sensor 22 and generates signals that represent tape position.

The directory controller 30 includes a microprocessor controller 31, a random access memory (RAM) 33 and a directory input/output display and control panel 32. Preferably the microprocessor controller 31 includes an integrated circuit microprocessor, and a program store, such as a read-only-memory (ROM), for storing a control program, and a clock for generating a clock signal for timing functions and providing the time. The time may be set using the directory input/output display and control panel 32 in a manner known in the art. Alternatively, the VCR 1 may maintain the time with clock 80. The RAM 33 is a conventional random access semiconductor memory which interfaces directly with the microprocessor controller 31. The RAM 33 is preferably non-volatile. Alternatively, the

RAM 33 is battery backed up. A portion of the RAM 33 is shown as 33b, which is used for storing the system software of the microprocessor controller 31. The RAM 33 is also used for storing the program directory 33a.

The directory input/output display and control panel 32 has an alphanumeric keyboard 32a and special function keys, such as a SEARCH key 32b for commanding searches for data in the directory 33a and on the tape 42, a MODIFY key 32c for modifying or deleting directory information in the RAM 33, and an ENTER key 32d for entering program directory information. Instead of providing special function keys, functions can also be initiated by entering predefined sequences of conventional keys on the alphanumeric keyboard 32a.

A display 32e is a conventional liquid crystal or other type display for displaying data being entered on the keyboard 32a, and to display the directory or other information stored in the RAM 33. Alternately, as discussed below, an on-screen display on video monitor 50a can be used. The directory information stored in the RAM 33 is processed by the microprocessor controller 31.

The VCR 1 additionally comprises a character generator circuit 23 coupled to the VCR control logic circuit 21 and to a character generator read-only memory (ROM) 25. Character generators are well-known in the art. Typically, the character generator ROM 25 stores a data table representing pixel or bit patterns of a plurality of alphanumeric characters, such as the Roman alphabet and the Arabic numerals. Upon command by the VCR control logic circuit 21 and the character generator circuit 23, the data in the character generator ROM 25 is read and placed in an output signal to the video monitor 50a at a position on the display determined by coordinates generated by the microprocessor controller 31. The end result is visual display of a alphanumeric character on the display screen. Character generators are well-known for on screen channel display in television receivers. The video monitor 50a is preferably 36 characters x 15 rows.

FIG. 1B is a block diagram of a transmitter in accordance with principles of the invention. The message body 84, which is described below, is encrypted and scrambled by encryption and scrambling unit 85. The encryption and scrambling are performed as a function of information in the header 86, which is further described below. Then header 86 and end code 88 are combined with the encrypted message body by combiner 90. Then the output of combiner 90 and a video program 82 are combined in combiner 92. The output of combiner 92, which is a composite video signal can be transmitted via antenna 96 or sent on a cable via cable output unit 94. The composite video signal can also be transmitted via satellite or telephone lines.

Television programs can include closed captions embedded in the program. This information can be embedded in the Vertical Blanking Interval (VBI) lines (described below) of a television video signal. A VBI decoder 60a in the VCR 1 or in a television is used to retrieve the closed captions from the VBI lines and then the closed captions are displayed as text on a video monitor.

Other information can also be embedded in the VBI lines. For example, a directory

)OCID: <WO___9517059A1_1_>

to programs can be embedded in the VBI lines. The directory can either be transmitted in the VBI lines during a transmission or stored in the VBI lines of a video cassette tape along with the programs on the video cassette tape. The directory can be then be used to control a video cassette recorder (VCR) to access programs on the video cassette tape. Such a system is described in application Serial No. 08/066,666, which is incorporated herein by this reference, as though set forth in full. Other information in the VBI lines can include channel specific program guide (CSPG), program related information (PRI), Instant Information (II), a V(M) packet, a TPA packet, which are described below.

For example a program title can be transmitted in the VBI lines along with a program which is being recorded on a VCR cassette tape. The VBI decoder can retrieve the program title from the VBI lines and then store the program title and the position of the start of the program in RAM 33 of directory controller 30 to assist the user in accessing the program in the future from the VCR cassette tape.

As discussed below the directory can be transmitted in a scrambled and encrypted form. The directory can be descrambled and decrypted before being stored in the RAM 33 or can be stored in RAM 33 in a scrambled and encrypted form.

As shown in FIG. 1A, VBI decoding can be implemented by coupling an input of a VBI decoder 60a to the output of a tuner 61, which is generally included in the majority of VCRs for tuning the VCR to a channel for off-the-air recording. The tuner 61 receives a TV signal from an antenna 63 or a cable TV signal source 64. Both the decoder, the tuner, and the interaction of both, are conventional in the art. Examples of commercially available VBI caption decoders include the TeleCaption 4000 Adaptor, commercially available from National Caption Institute, Falls Church, Virginia, the Teletext Decoder, available from Norpak Corporation, Ottawa, Canada, and the VBI Decoder CCD3000 available from ITT Semiconductor.

A decoder signal line 65 is coupled from the decoder to the VCR control logic circuit 21. The VCR control logic circuit 21 may be commanded by the microprocessor controller 31 to pass the decoded data to the directory 33a under control of a stored program in the RAM 33. For example, if the VBI data includes a program title, then the program causes the VBI information to be stored as a program title in the directory 33a. On command from a user, the directory contents are displayed on the video monitor 50a and the user can select a program to access by using keyboard 32a.

Vertical Blanking Interval Lines

FIG. 2 is a diagram illustrating the fields, frames and vertical blanking interval of an interlaced television scanning raster 100. The first field 102 of the television signal starts at the upper left corner of the screen and writes lines 21, 22, .. 263. At the bottom of the screen the beam writing the screen retraces in a series of lines back to the top of the screen. These lines are shown as the vertical blanking interval lines 106. During the retrace the writing to the screen is blanked; however, because the signal is still present, additional information can be sent during the vertical blanking interval. There are at least 20 lines in the vertical blanking interval, and it is possible to have additional VBI lines. After the

vertical blanking interval, the second field 104 is written on the screen and lines 283, 284, . . . 525 are interleaved between the lines of the first field 102. The two fields and the vertical blanking interval together constitute a frame. FIG. 3 is a diagram illustrating the timing 110 of the vertical blanking interval (VBI) lines 1 to 20. As shown each vertical blanking interval line 111 occupies a portion of the time span. Each VBI line, such as 19 as shown in FIG. 3, can contain 2 to 4 bytes of information. When a message is embedded in the VBI lines the message is typically longer than 2 to 4 bytes and is spread across a number of fields and frames. Closed caption data 112 and extended data services (EDS) data 116 can be embedded in VBI lines. The information contained in a VBI line can include a channel specific program guide (CSPG), program related information (PRI), Instant Information (II), a V(M) packet, a TPA packet, or a directory, as indicated by element 114 in FIG. 3.

Recorded Tapes with Information in the VBI Lines

FIG. 4 is a schematic of recorded tapes illustrating storing Video Index Search System (VISS) marks on a control track, TPA packets each containing a tape identification number, a program number, and an absolute address in vertical blanking interval lines, and a directory stored in the vertical blanking interval lines in accordance with principles of the invention. In FIG. 4 VISS marks 186, 188 and 190 are placed in the control track 166 at the start of the programs. This can be done at the time the tape is produced or copied from a master tape. On a pre-recorded tape the TPA packets 176 and directory 178 are also previously stored onto the tape on vertical blanking interval lines 19 and 20, respectively, which are designated as 167 and 168 in FIG. 4.

Each TPA packet 215 contains a tape identification 214, a program number 216 and an absolute address 218, as shown in FIG. 5A. The tape identification is a number that identifies the video cassette tape being used and is constant across the tape. The program number relates to the number of the program that is recorded on the tape adjacent to the TPA packet. For example, the TPA packets shown in FIG. 4 as TP_3A, correspond to program number 3. The absolute address in the TPA packet is an indication of the time (or distance) from the beginning of the tape to the location on the tape at which the particular TPA packet is written. Since the TPA is written in VBI lines across the tape, the absolute address varies across the tape. The TPA packet may also contain a month and year field 220, the use of which is described below.

Each directory entry is used to store information about a program stored on the recording tape. For example, a directory may contain for a program: the program title 205, the program number 206, the start address 208, the end address 210 and the record speed 212, as shown in FIG. 5B. Additional fields 204 can be provided to allow room for expansion. In particular the additional field can include fields for program category (PC), version, and language.

The TPA packets and the directory information can be used along with the VISS marks for accessing programs on the tape. The directory on the tape is accessed and stored in directory 33a and displayed to a user, who can then select a program to view. The VCR will

DOCID: <WO__9517069A1_I_>

then access the program using the information in the TPA packets stored along the tape and the information in the directory. By comparing the start address of the program in the directory with the absolute address in the TPA packet it can be determined whether to advance or rewind the tape to access the beginning of the selected program, which is marked by a VISS index mark. Then the program can be played by the VCR. The method of accessing programs on a pre-recorded tape is further described in U.S. patent application serial number 08/167,285, filed 12/15/93, which is incorporated herein by this reference, as though set forth in full.

As described in U.S. patent application serial number 08/167,285, filed 12/15/93, TPA packets and VISS marks can be recorded on home recorded tapes to assist in accessing programs on a tape. In the case of home recorded tape the directory is retained in RAM 33 rather than in a VBI line.

Information Transmitted in the VBI Lines

The types of information that can be transmitted in a VBI line include: a channel specific program guide (CSPG), program related information (PRI), Instant Information (II), a V(M) packet, TPA packet, and a directory, as indicated by element 114 in FIG. 3.

The format for transmitting the information in a VBI line is shown in FIG. 6. This same format applies to channel specific program guide (CSPG), program related information (PRI), Instant Information (II), V(M) packets, TPA packets, and directories that are transmitted in a VBI line. The transmission begins with a header 242 that includes a start code 248, a type code 250, and a message ID 252. The type code indicates the type of message. The message ID can be used to identify a message.

The header 242 is followed by the body 244, which contains the information of the message. The body 244 can contain a CSPG, a PRI, an II, V(M) packets, TPA packets, or a directory.

The CSPG is the combination of the program information for a plurality of programs that will be transmitted in an upcoming predetermined time on a particular channel. The information for each program may include:

- Title of program
- Program length in minutes
- Day and time of day of transmission
- Station call letters (e.g. KCET or KCAL) or 4-letter abbreviation of station name (e.g. SHOW for Showtime)
- Channel number

In addition to the above information, the channel specific program guide may also include compressed code numbers representing a channel, date, time and length. Also a description of the programs can be included.

Program related information (PRI), which can also be referred to as Instant Information (II), is information transmitted in the VBI that is related to a program being broadcasted which is available upon user command either concurrently with the program or at a later time. When PRI or II is broadcast, the user is prompted and the user can respond

with a command to retrieve the PRI or II and either display the PRI or II or perform other appropriate steps related to the PRI or II. If the PRI or II is encrypted or scrambled then it is first decrypted and descrambled. Examples of PRI include statistics of baseball players during a baseball game, recipes given out during a cooking lesson, and problem assignments and answers after an educational program. The PRI or II can also include a date, time, channel and length of a program to be broadcast at a later time. In this case when the user responds to the prompt that PRI or II is available, then a VCR is programmed automatically to record the program broadcast at a later time.

V(M) packets transmitted in the VBI can be used to mark the beginning of sections of a video magazine or used to mark the beginning of a program.

The TPA packet and directory information and their use for accessing recorded programs have been described above.

Following the body 244 is the end 246, which contains a stop code 254 and a checksum 256.

When the directory and the TPA packets are written in the VBI of a tape, as shown in FIG. 4 and discussed above, the directory and/or the TPA packets can be encrypted or unencrypted.

Encrypting Information in VBI Lines

Now that the types and formats of the information have been described, the methods for encryption and decryption of the information will be discussed. The purpose of encrypting the information is to protect against unauthorized access of the information.

In general messages embedded within a vertical blanking interval are encoded by generating a key dependent on time and the message and then using the key to select a table or tables for mapping portions of the message into an encrypted message. The method of encryption applies to messages that are transmitted, and to information that is stored on a recorded tape in the VBI lines. In digital tapes it is not necessary to use VBI lines because there is an area of tape available for the information. The methods of encryption and decryption described herein are equally applicable to information that is recorded on a digital tape.

FIG. 8A is a flowchart of a method for encrypting information embedded in a video program that is transmitted according to principles of the present invention. The method of FIG. 8A can be implemented by a program for a microprocessor or a computer at the transmitter. A message to be transmitted is shown as element 240 in FIG. 8A and corresponds to element 240 of FIG. 6. As shown the message consists of a start code, type and message ID that constitute the header of the message. The body of the message, which can be either CSPG, PRI, II, a V(M) packet or a directory, follows the header. The end field, which includes a stop code and a checksum, follows the body. The body of the message is the portion of the message that needs to be protected with encryption.

Shown in FIG. 8B are directory 204 and TPA packet 215, which represents information to be recorded on a tape.

First, the encryption of the body of the message to be transmitted of FIG. 8A will be

OCID: <WO__9517068A1_1_>

described and then any modifications for encrypting information that is to be recorded on a tape, as shown in FIG. 8B will be described.

In step 306 the odd/even bit of the message ID is inspected to determine whether it is a zero or a one. As shown in FIG. 6 the message ID includes an odd/even bit. If the odd/even bit is zero then the month is an odd month. If the odd/even bit is a one then the month is an even month. The odd/even bit is further described in FIG. 7. As shown in FIG. 7 the odd/even bit retains its value over a period of two months. For example, as shown the odd/even bit might be zero during the months of May and June. The reason the odd/even bit is zero for the months May and June is that the two month period begins during the month of May which has an odd number 5. The odd/even bit 260 in FIG. 7 is one spanning the months of June and July. In this case the odd/even bit is a one because the beginning month June is represented by the numeral 6 which is even. So the odd/even bit value is determined by whether the first month of a pair of months is odd or even.

The reason to have an odd/even bit is that if a transmission is near the transition between May and June then the transmitter may believe that the month is May however, the receiver, for example, a VCR may, according to its internal clock think that it is the month of June. Suppose this is the case. If the VCR clock indicates June of 1993 and the odd/even bit is zero then the VCR will know that the transmitter believes that it is May because the odd/even bit has been set to zero. However, if the odd/even bit is a one then the VCR will know that the transmitter is transmitting in the month of June.

So in step 306 the first step is to inspect the odd/even bit to determine whether it is a zero or a one. Note that when transmitting the odd/even bit can be set by the transmitter to either be a zero or a one. If the odd/even bit has been set to a zero then in step 308 if the date of transmission is odd then the next step for a transmission is step 316. On the other hand, if the date of transmission as tested in step 308 is even then for a transmission the next step is 314. In step 316 a key is generated based on the month and year of the current month of transmission and based on the message ID. In step 314 a key is generated based on the date of the month previous to the month of transmission and based on the message ID. For example, suppose the odd/even bit is set to zero to indicate odd and suppose the month and year of transmission is June of 1993, then the key will be generated based on the date of May 1993 as indicated in step 314.

There are many ways in which the key can be generated based on the month and year of transmission. For example, the month can be added or subtracted from the year, or the concatenation of the month and year can be added to the message ID and a remainder module 32 calculated.

Once the key is generated then in step 320 the key is used to look up a second key in a table. Then in step 322 the second key is used to select a table for encrypting the bytes of the body of the message in step 324. Once the bytes are encrypted then in step 326 the start code, type, message ID, encrypted body, stop code and checksum are concatenated together to form the encrypted message to be transmitted.

FIG. 10 illustrates the manner of encrypting the bytes of the body of the message. For

example, suppose a bit of the body is 22 HEX as shown as element 404 in FIG. 10. The value 22 HEX is used as an address to a table 402 to look up a substitute byte, in this case 53 HEX, designated as element 406 in FIG. 10. As an additional encryption step the looked up value 53 HEX can then be used as an address to a second table 408 to look up another substitute value, in this case 7A HEX designated as element 410 in FIG. 10. The original byte of a body has one bit of parity and after the table lookup another parity bit can be added in step 412 to produce an encrypted body byte 414. Note that in table 402 the values in the table from 00 through 1F HEX are mapped into the same values. This also applies to the first entries in table 408. By not changing the mapping of the lower order entries in the table the method of encryption is more difficult to determine.

The method of FIG. 8B for encrypting information recorded on a tape such as a directory as shown in element 204 of FIG. 8B, is similar to the encoding of the body 244 of the message 240 of FIG. 8A. The method of FIG. 8b can be implemented by a program for a microprocessor or a computer. In the case of FIG. 8B, an odd/even bit is stored as a portion of the tape identification field as shown as element 219 in FIG. 5A. In step 306 the odd/even bit is examined to determine whether it is a zero or a one. Again, as in the case of an encryption for a transmission, the odd/even bit can be selected to be either zero or one. Then in steps 308 and 310 the month and year that the directory is recorded into the tape is inspected to determine whether the month is a odd or even month. If the month is determined to be odd in step 308 then the next step is step 318, and if it is determined to be even in step 308 then the next step is 312. Similarly, if in step 310 the month is determined to be odd then the next step is 312 and if the month is determined to be even then the next step is 318. In step 312 a key is generated based on the date of the month previous to the month of recording. The key can also be a function of the tape ID. In step 318 a key is generated based on the date of the month of recording and can also be a function of the tape ID. The key that is generated is used in step 320 and step 322 to select tables for encrypting bytes of the directory. This can be done in the manner described in FIG. 10. Then in step 328 the encrypted directory is written into the VBI lines. Also the month and year of recording the encrypted directory is written into the TPA packet as shown in element 220 of FIG. 5A. The entire TPA packet 215 can be encrypted in the same manner.

The key based on the month and the tape ID can be generated in the same manner as indicated for steps 314 and 316.

When a message is received it must be decrypted. FIG. 9A is a flowchart of a method for decrypting information embedded in a video program that is transmitted according to principles of the present invention. The method of decrypting shown in FIG. 9A can be implemented by a microprocessor realization of VCR control logic 21 or by VBI decoder 60a. Element 326 of FIG. 9A, which corresponds to element 326 of FIG. 8A, shows an encrypted body of a message. In step 364 the odd/even bit contained in the message ID of the message 326 is examined to determine whether the odd/even bit is a zero or one. If the odd/even bit is a zero then in step 366 the clock 80 of the VCR is examined to determine whether the VCR clock is at a month which is odd or even. If the clock 80 month is an odd

XOCID: <WO__9517059A1_1_>

month then the next step is step 374 and if the clock 80 month is even then the next step is step 372. If the odd/even bit is a one then if the clock 80 month is odd as determined in step 368 the next step is 372 and if the clock 80 month is an even month then the next step is step 374. In step 372 a key is generated based on the date of the month previous to the month on the clock 80 and can also be generated as a function of the message ID. In step 374 the key is generated based on the date of the current month on the clock 80 and can also be generated as a function of the message ID. The method of generating the key based on the month and the message ID can be as indicated for steps 314 and 316 above. After the key is generated then in step 378 the key is used to look up a second key in a table which is then used to select a table or tables for decrypting bytes in step 380. In step 382 the tables for decrypting bytes are used to decrypt each byte.

FIG. 11 is an illustration of the method of mapping encrypted bytes of a body to decrypted bytes according to the present invention. As shown in FIG. 11 the encrypted byte 420 is used as an address to table 424. For example, if byte 420 is 7A HEX then this is used as an address and the output of table 424 is 53 HEX which is represented as element 426 in FIG. 11. This output of table 424 can then be used to look up another substitute byte in table 428 and in this case 22 HEX is the output of table 428. Then in step 432 the parity bit is added to the output of the table 428 to complete the mapping of encrypted body byte 420 to decrypted body byte 434.

In step 384 the decrypted body is recorded onto the VCR tape. In step 386 VCR clock 80 value for the month and the year and the odd/even bit from the message ID is recorded onto the VCR tape into the TPA packet as shown in FIG. 5A.

The method for decrypting an encrypted directory that has been recorded onto the tape as indicated in element 328 of FIG. 9B, which corresponds to element 328 of FIG. 8B, is similar to the decryption of the encrypted body of element 326 of FIG. 9A. The method of FIG. 9B can also be implemented by a microprocessor. The key difference is that step 376 is substituted for step 374 and step 370 is substituted for step 372. In step 370 a key is generated based on the month previous to the month that is in the TPA packet of element 328 and can also be generated based on the tape ID. In step 376 the key is generated based on the date of the month in the TPA packet of element 328 and can also be based on the tape ID. The key that is generated is again used to look up another key in step 378 and then to select tables 382 for decrypting the bytes in step 380. The result is a decrypted directory 388. An example of the encryption and decryption will now be given.

For a message that is transmitted, suppose the original message is: "The red fox ran over the fence." Suppose the year and month of transmission is June of 1993 and suppose the odd/even bit is set to be odd. Since the odd/even bit is odd and the year and month of transmission is June of 1993 the key for encrypting the message will be based on May of 1993. After encoding according to FIG. 8., the encrypted message is funsieu3l;lnfEidpak;auefa-ue;faie. The VCR 1 then receives the encrypted message. If the month and year of VCR clock 80 is June of 1993, then when the VCR reads the odd/even bit from the message ID and determines it is odd then the key will be generated based on

May of 1993. The decrypted message will be ""The red fox ran over the fence." As a second example, suppose that the encrypted message is recorded on a tape and suppose that the month and year in VCR clock 80 is December 1993, suppose the year and month recorded in the TPA packet on the tape is June of 1993 and suppose the odd/even bit recorded in the TPA packet is odd. Then when the VCR 1 decrypts the encrypted message it will generate a key based on May of 1993. The decrypted message will be "The red fox ran over the fence."

Alternate Method of Encrypting/Decrypting

In an alternate embodiment the encryption and decryption is performed using a secret key encrypto-system such as the data encryption standard (DES) proposed by IBM and adopted by NBS in 1978.

Scrambling/De-scrambling of Data

After encryption, the encrypted data can be scrambled by using a scrambling key to swap the bits of the encrypted data. The scrambling key is preferably a predetermined set of numbers that are selected from a number that is associated with the data transmitted in the VBI or recorded in the VBI on tape. For example, for prerecorded tapes, a predetermined number of bits of the tape identification number are used as a key. For example, seven bits, such as bits 22-28, of the tape identification number may be used. The tape manufacturer uses these bits to scramble the data recorded on the tape. In the VCR 1, the tape identification number 214 is read from the VBI and the predetermined set of bits are used to de-scramble the encrypted data. As a second example, for transmitted information, a predetermined number of bits of the type data 250 are used as a key. For example, four bits of the type data 250 may be used. The manufacturer of a master tape used by the transmitter or the transmitter itself may use these bits to scramble the data. The indexing VCR 1 reads the type data from the transmitted VBI and retrieves the predetermined set of bits as a key. The indexing VCR 1 then uses this key to descramble the transmitted data.

One example of scrambling and de-scrambling is to apply the 7 bits to pairs of alpha numeric characters in the data and depending upon whether the bit is one or a zero, swap the characters. For example, where a one digit appears the characters of the pair are swapped, where a zero appears, the characters are not swapped. For example, for a seven bit sequence of 1011001, the phrase CHRISTIE PARKER HALE becomes scrambled by switching the C and H of the first character pair to read HC for the first one in the seven bit sequence. The RI is not swapped because the second bit is a zero; the ST is swapped to TS because the third bit is a 1; the IE is swapped to read EI because the fourth bit is 1; and so forth. In addition, the pattern is repeated for each set of seven pairs. Spaces are included as a character. Thus, CHRISTIE PARKER HALE becomes HCRITSEI PAREK RHAEL. By applying the same seven bit sequence 1011001, the character sequence can be de-scrambled.

DOCID: <WO__9517059A1_1_>

Since after encryption the body portion is scrambled, then before decryption the body portion must first be de-scrambled. It is also possible to perform scrambling before encryption, which requires de-scrambling before decryption. Both of these combinations are within the scope of the invention.

The described embodiments of the invention are only considered to be preferred and illustrative of the inventive concept, the scope of the invention is not to be restricted to such embodiments. Various and numerous other arrangements may be devised by one skilled in the art without departing from the spirit and scope of this invention.

It is therefore intended by the appended claims to cover any and all such applications, modifications and embodiments within the scope of the present invention.

WHAT IS CLAIMED IS:

1. A method for transmitting information having a header portion and a body portion comprising the steps of:

providing a clock having an output as a function of time;

generating a first key based on the time from the clock and a part of the header portion;

using the first key for encrypting the body portion to generate an encrypted body portion;

combining the encrypted body portion and the header portion to form a data packet;

combining a video program and the data packet to form a composite video signal; and

transmitting the composite video signal.

2. A method for recording information having a body portion and a header portion on a video cassette tape comprising the steps of:

providing a clock having an output as a function of time;

generating a first key based on the time from the clock and a part of the header portion;

using the first key for encrypting the body portion to generate an encrypted body portion;

embedding the encrypted body portion and the header portion within a video program to form a composite video signal; and

recording the composite video signal on a video cassette tape.

3. The method of Claim 1 or 2 further comprising the steps of:

generating a scrambling key from a part of the header portion;

scrambling the encrypted body portion using the scrambling key; and

embedding the encrypted and scrambled body portion and the header portion within a video program to form a composite video signal.

4. The method of Claim 3 wherein the scrambling key comprises a binary form having bits of either a first or second type, and the method further comprises the steps of:

(a) applying each bit of the scrambling key to a predetermined number of pairs of characters in the encrypted body portion;

(b) swapping the characters of the pair if the assigned bit is of a first type;

(c) otherwise, not swapping the characters of the pair if the assigned bit is of a second type; and

repeating the steps (a)-(c) for all pairs of characters of the encrypted body portion.

XOCID: <WO__9517059A1_1_>

5. The method of Claim 1 or 2 wherein the step of generating a first key based on time from the clock and a part of the header portion comprises the step of generating the first key based on the month and year from the clock.

6. The method of Claim 5 wherein the step of using the first key for encrypting the body portion to generate an encrypted body portion comprises the step of:

using the first key to select a first table;

mapping each part of the body portion to a first encrypted part using the first table; and

concatenating each encrypted part to form an encrypted body portion.

7. The method of Claim 6 wherein each part of the body portion comprises a byte.

8. The method of Claim 7 wherein the step of mapping each part of the body portion to a first encrypted part using the first table comprises the steps of:

using the first key to select a second table; and

mapping each first encrypted part to a second encrypted part using the second table.

9. The method of Claim 8 wherein the step of generating the first key based on the month and year from the clock comprises the step of using the first key to look up a second key in a third table.

10. The method of Claim 9 wherein the step of generating the first key based on the month and year from the clock comprises the steps of:

providing an odd/even month indication in the header portion;

if the odd/even month indication is odd and the month from the clock is an even month or if the odd/even month indication is even and the month from the clock is an odd month then generating the first key based on the month previous to the month and year from the clock; and

if the odd/even month indication is odd and the month from the clock is an odd month or if the odd/even month indication is even and the month from the clock is an even month then generating the first key based on the current month and year from the clock.

11. The method of Claim 1 wherein the step of combining a video program and the data packet to form a composite video signal comprises the step of embedding the data packet in the vertical blanking interval lines of the video program.

12. The method of Claim 2 wherein the step of embedding the encrypted body portion and the header portion within a video program to form a composite video signal comprises the step of embedding the encrypted body portion and the header portion in the vertical blanking interval lines of the video program.

13. A method for receiving transmitted information having a header portion and an encrypted body portion, the method comprising the steps of:

providing a clock having an output as a function of time;

generating a first key based on the time from the clock and a part of the header portion;

using the first key for decrypting the encrypted body portion to generate an decrypted body portion;

combining the decrypted body portion and the header portion to form a data packet; and

recording the data packet on a video cassette tape.

14. A method for decrypting recorded information having a header portion and an encrypted body portion, the method comprising the steps of:

providing a clock having an output as a function of time;

generating a first key based on the time from the clock and a part of the header portion; and

using the first key for decrypting the encrypted body portion to generate a decrypted body portion.

15. The method of Claim 13 or 14 further comprising the steps of:

generating a de-scrambling key from a part of the header portion; and

de-scrambling the encrypted body portion using the de-scrambling key.

16. The method of Claim 15 wherein the de-scrambling key comprises a binary form having bits of either a first or second type, and the method further comprises the steps of:

(a) applying each bit of the de-scrambling key to a predetermined number of pairs of characters in the encrypted body portion;

(b) swapping the characters of the pair if the assigned bit is of a first type;

(c) otherwise, not swapping the characters of the pair if the assigned bit is of a second type; and

repeating the steps (a)-(c) for all pairs of characters of the encrypted body portion.

17. The method of Claim 13 or 14 wherein the step of generating a first key based on time from the clock and a part of the header portion comprises the step of generating the

DOCID: <WO__9517059A1_I_>

first key based on the month and year from the clock.

18. The method of Claim 17 wherein the step of using the first key for decrypting the encrypted body portion to generate a decrypted body portion comprises the steps of:

using the first key to select a first table;

mapping each part of the encrypted body portion to a first decrypted part using the first table; and

concatenating each decrypted part to form a decrypted body portion.

19. The method of Claim 18 wherein each part of the encrypted body portion is a byte.

20. The method of Claim 19 wherein the step of mapping each part of the encrypted body portion to a first decrypted part using the first table comprises the steps of:

using the first key to select a second table; and

mapping each first decrypted part to a second decrypted part using the second table.

21. The method of Claim 20 wherein the step of generating the first key based on the month and year from the clock comprises the step of using the first key to look up a second key in a third table.

22. The method of Claim 19 wherein the step of generating the first key based on the month and year from the clock comprises the steps of:

receiving an odd/even month indication embedded in the header portion;

if the odd/even month indication is odd and the month from the clock is an even month or if the odd/even month indication is even and the month from the clock is an odd month then generating the first key based on the month previous to the month and year from the clock; and

if the odd/even month indication is odd and the month from the clock is an odd month or if the odd/even month indication is even and the month from the clock is an even month then generating the first key based on the current month and year from the clock.

23. The method of Claim 19 further comprising the steps of:

recording the received odd/even month indication on a video cassette tape; and

recording the output of the clock on the video cassette tape.

24. A method for broadcasting information comprising the steps of:

generating data containing the information;

generating a header related to the information;

generating a scrambling key from a portion of the header;

scrambling the data using the scrambling key to generate scrambled data;
combining the scrambled data and the header to form a data packet;
generating a video program;
combining the video program and the data packet to form a video signal; and
transmitting the video signal.

25. The method of claim 24 wherein the data packet is broadcast in the vertical blanking interval of the video signal.

26. The method of claim 24 wherein the scrambling key comprises a binary form having bits of either a first or second type, and the method further comprises the steps of:

(a) applying each bit of the key to a predetermined number of pairs of characters in the data;

(b) swapping the characters of the pair if the assigned bit is of a first type;

(c) otherwise, not swapping the characters of the pair if the assigned bit is of a second type; and

repeating the steps (a)-(c) for all pairs of characters of the data.

27. The method of claim 26 wherein the first type is a one and the second type is a zero.

28. A method for recording information on a video tape comprising the steps of:
generating a tape identification number;
generating a directory data packet, the directory data packet having directory information;
generating a scrambling key from a portion of the tape identification number;
scrambling the directory information using the scrambling key to generate a scrambled directory data packet;
generating a plurality of video programs;
combining the plurality of video programs and the scrambled directory data packet to form a video signal; and
writing the video signal on the video tape.

29. A video tape comprising:
a recording medium having a plurality of video frames;
a plurality of video programs recorded on the video tape; and
a directory containing information related to the video programs, a first portion of the information being scrambled using a scrambling key generated from a second portion of the information, the directory being recorded in the vertical blanking interval of the video programs on the tape.

OCID: <WO___9517059A1_L>

30. The video tape of claim 29 wherein a second portion of the information comprises a tape identification number.

31. A method for descrambling data comprising the steps of:

detecting video signals containing video programs and information, the information having a first portion of unscrambled information and a second portion of scrambled information;

generating a descrambling key from the first portion of unscrambled information; and

applying the descrambling key to the second portion of scrambled information to generate unscrambled information.

32. The method of claim 31 where the step of detecting video signals comprises the step of detecting video signals from a broadcasted signal.

33. The method of claim 31 wherein the first portion comprises a tape identification number.

34. The method of claim 33 wherein the step of detecting video signals comprises the step of reading video signals from a recorded tape.

35. A method for retrieving data containing information related to a broadcasted video program comprising the steps of:

detecting the data in a video signal;

decrypting the data to form decrypted data;

displaying in temporal proximity to the broadcasted program a prompt on a television screen informing a user that information related to the broadcasted video program is available;

detecting user selection commands; and

responding to the detected user commands.

36. The method of claim 35 wherein the decrypted data comprises timer programming information for a second program to be broadcast at a later time, and the step of responding to the detected user commands comprises the step of timer programming a video cassette recorder to record the second program.

37. The method of claim 36 wherein the timer programming information comprises the date, time, channel, and length of the second program.

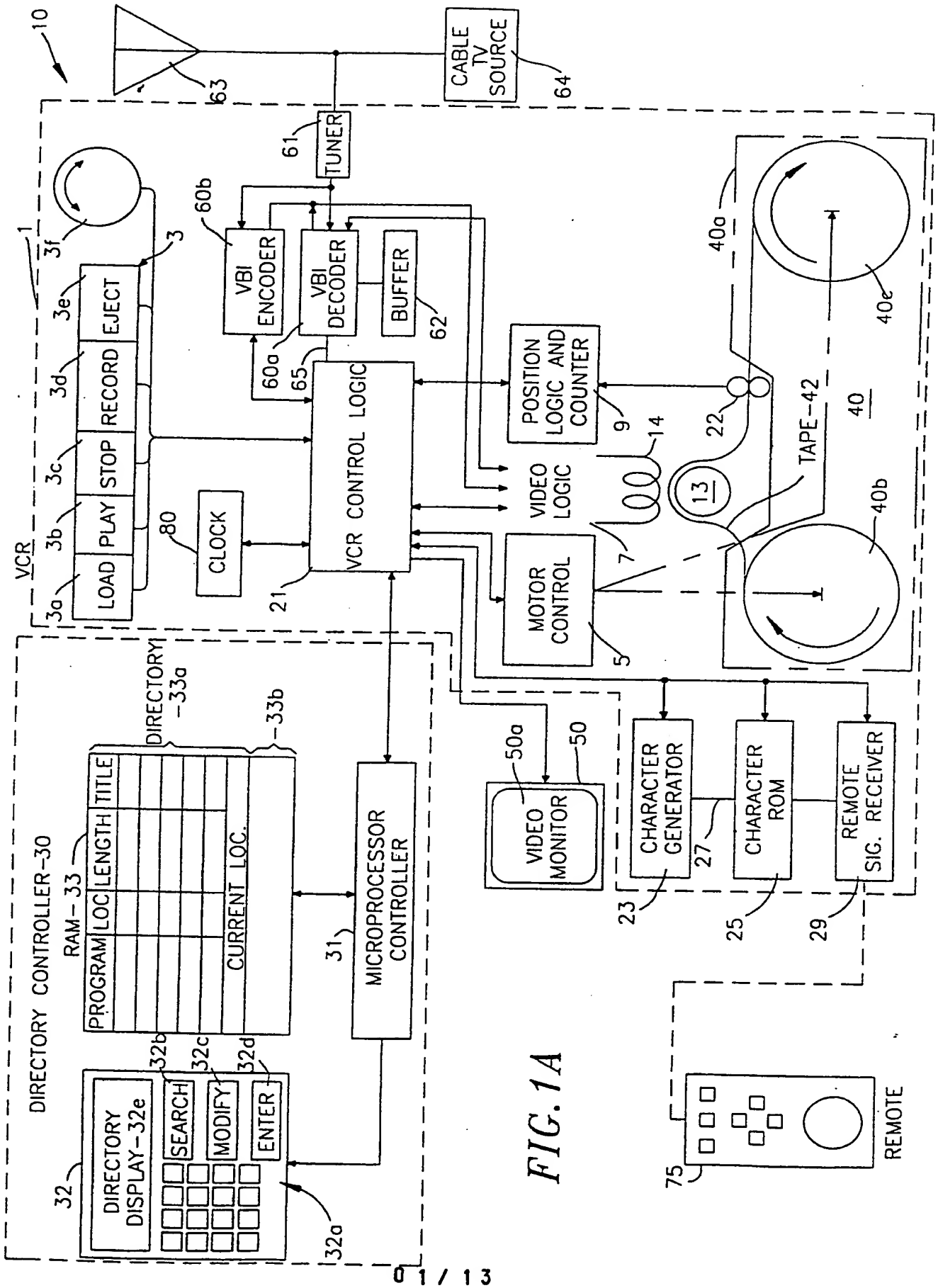


FIG. 1A

XOCID: <WO__9517069A1_I_>

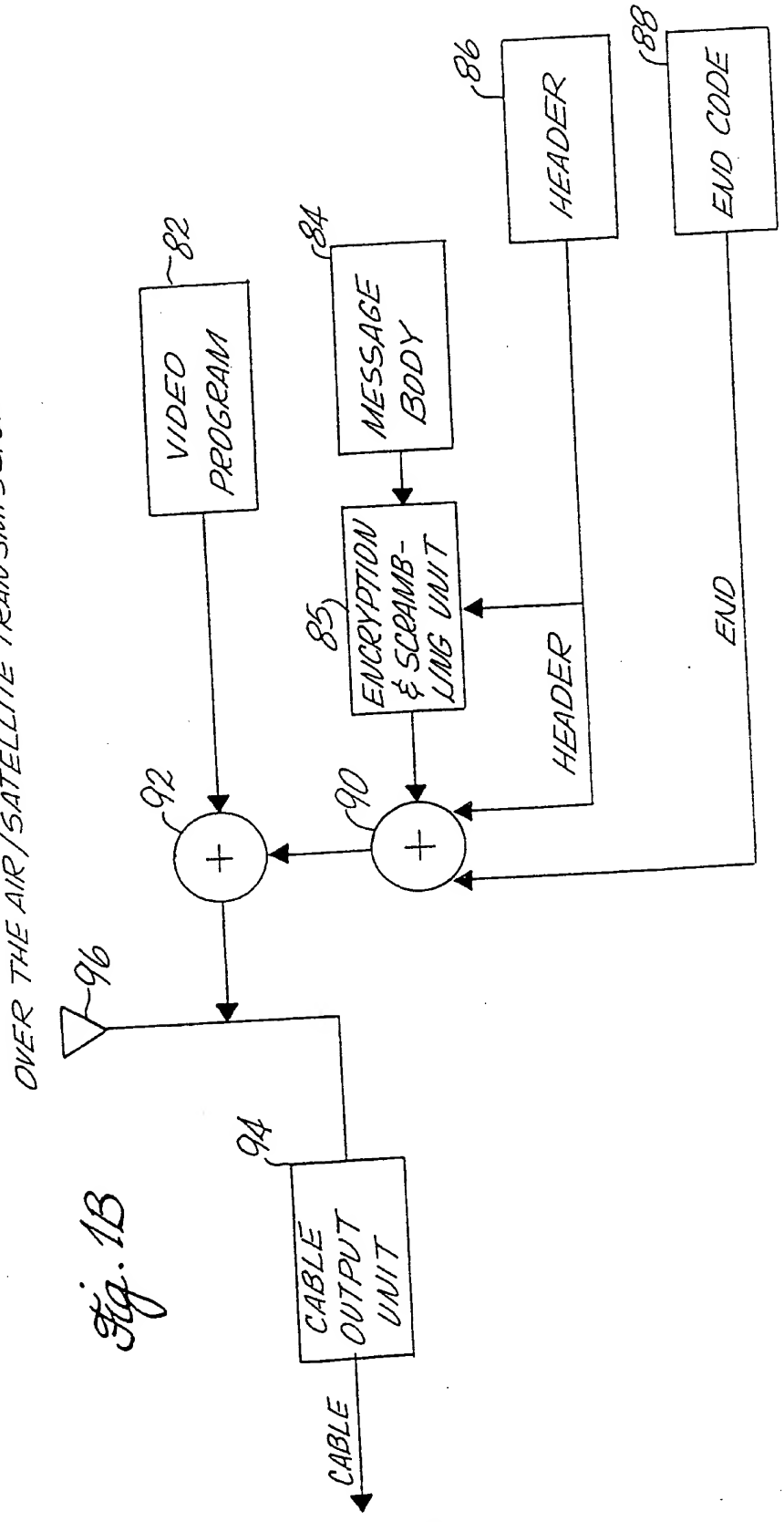

VIDEO PROGRAM
82
MESSAGE BODY
84
HEADER
86
END CODE
88
ENCRYPTION & SCRAMBLING UNIT
85
HEADER
END
92
90
OVER THE AIR/SATELLITE TRANSMISSION
96
CABLE OUTPUT UNIT
94
CABLE

Fig. 1B

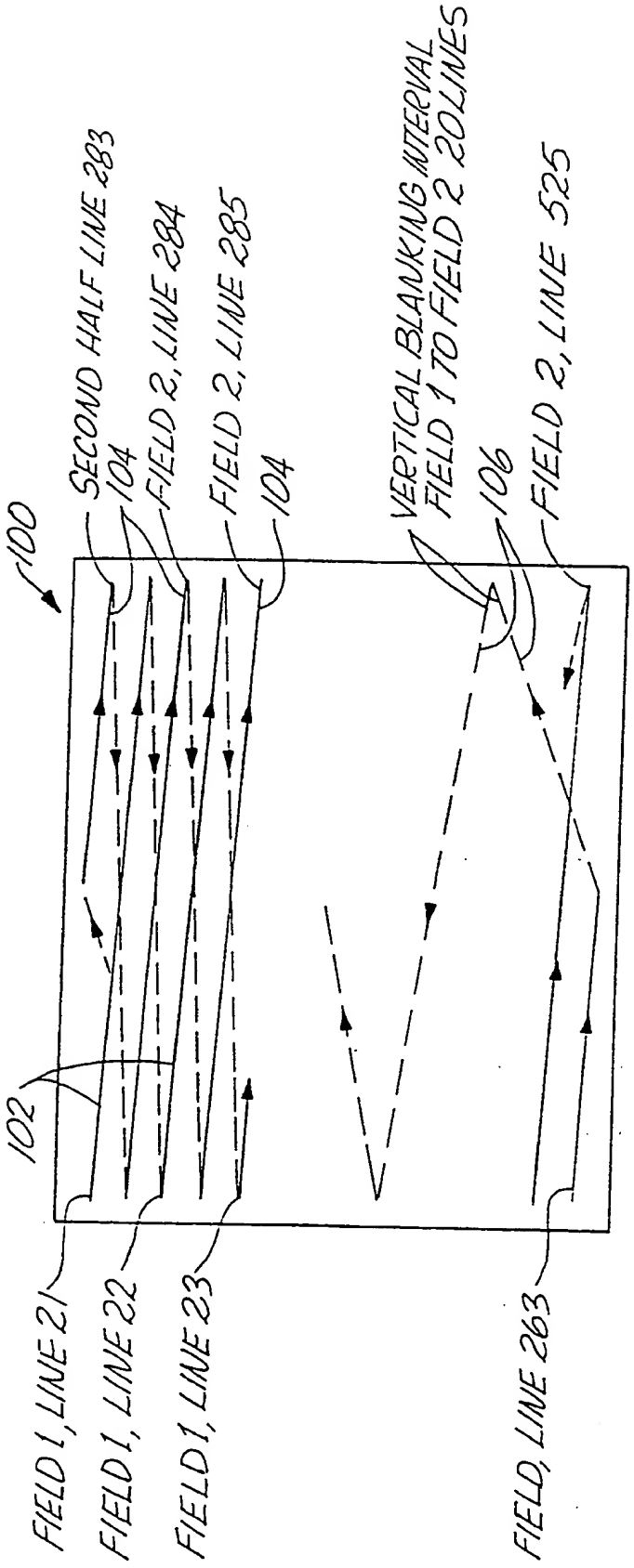


Fig. 2
PRIOR ART

DCID: <WO___9517059A1_I_>

Fig. 3

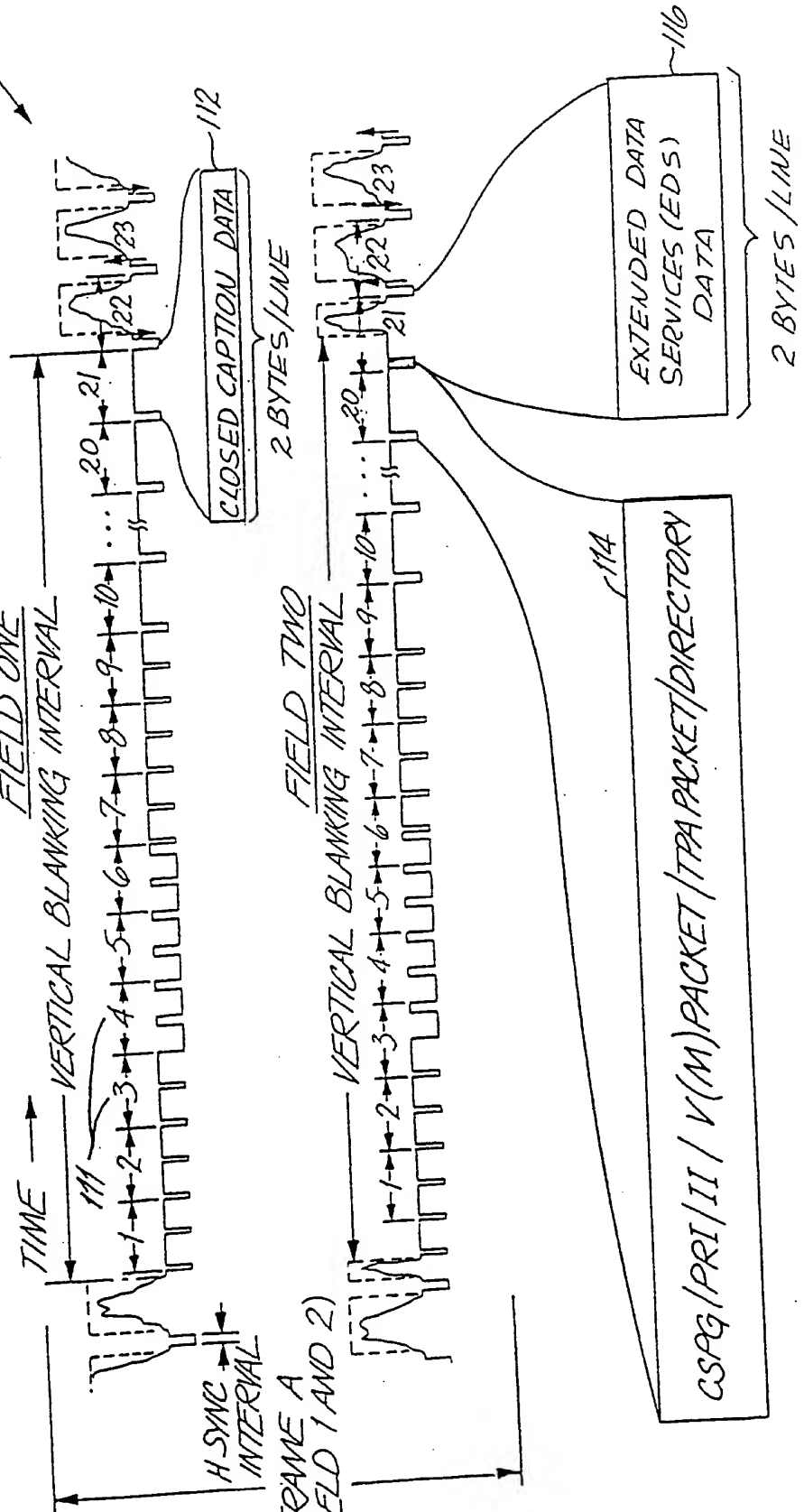
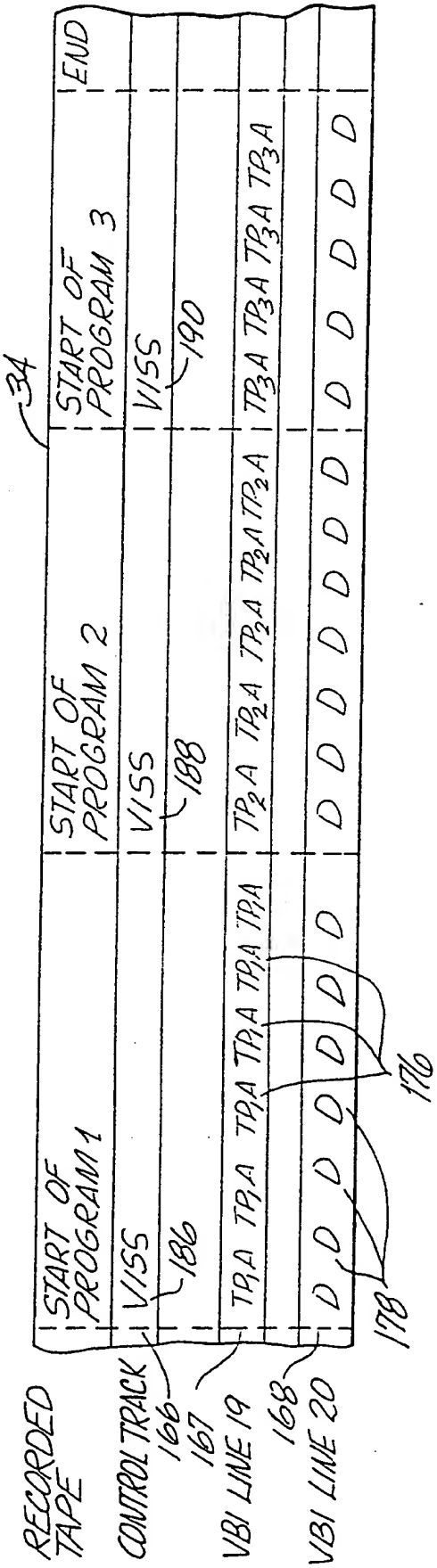

110
FIELD ONE
VERTICAL BLANKING INTERVAL
TIME
111
1
2
3
4
5
6
7
8
9
10
20
21
22
23
112
CLOSED CAPTION DATA
2 BYTES/LINE
H SYNC INTERVAL
FRAME A (FIELD 1 AND 2)
FIELD TWO
VERTICAL BLANKING INTERVAL
11
116
EXTENDED DATA SERVICES (EDS) DATA
2 BYTES/LINE
114
CSPG/PRI/II / V(M)PACKET/TPA PACKET/DIRECTORY

Fig. 4



OCID: <WO___9517059A1_1_>

Fig. 5A

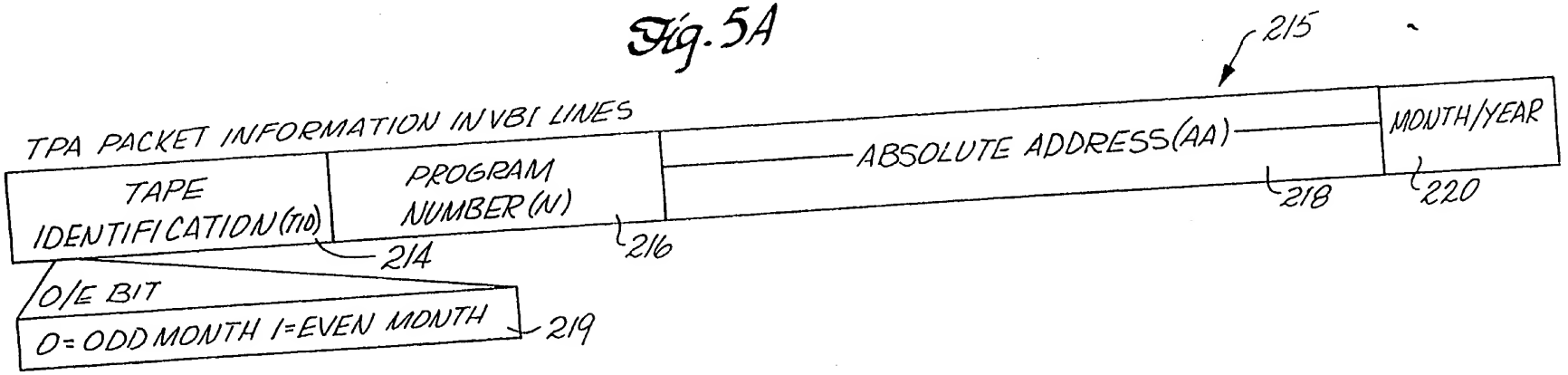
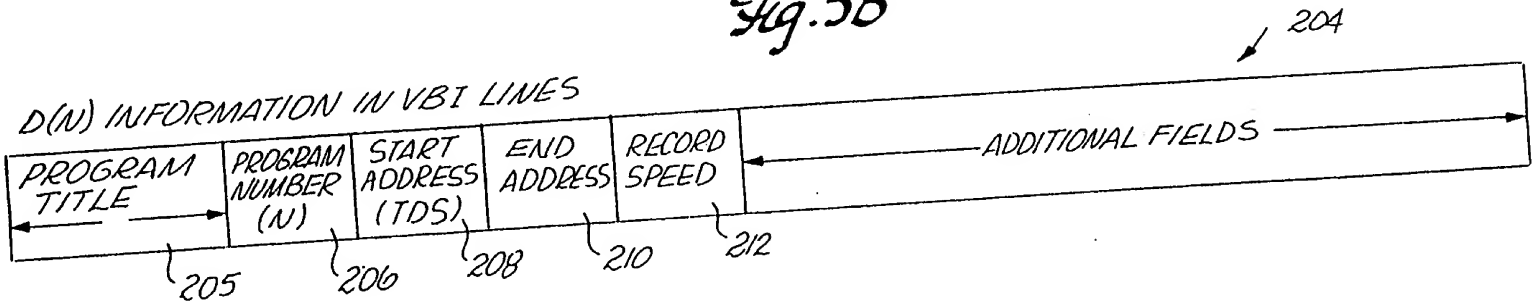

TPA PACKET INFORMATION IN VBI LINES
TAPE IDENTIFICATION (TID)
PROGRAM NUMBER (N)
ABSOLUTE ADDRESS (AA)
MONTH/YEAR
215
214
216
218
220
O/E BIT
O = ODD MONTH 1 = EVEN MONTH
219

Fig. 5B


D(N) INFORMATION IN VBI LINES
204
PROGRAM TITLE
PROGRAM NUMBER (N)
START ADDRESS (TDS)
END ADDRESS
RECORD SPEED
ADDITIONAL FIELDS
205
206
208
210
212

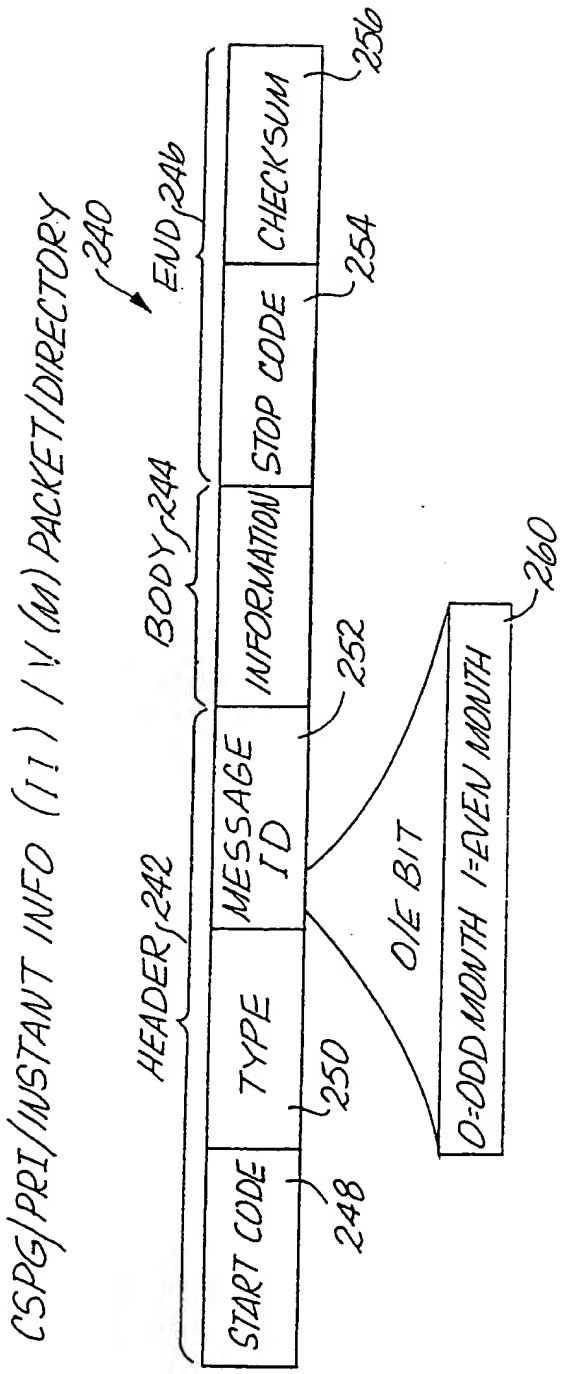
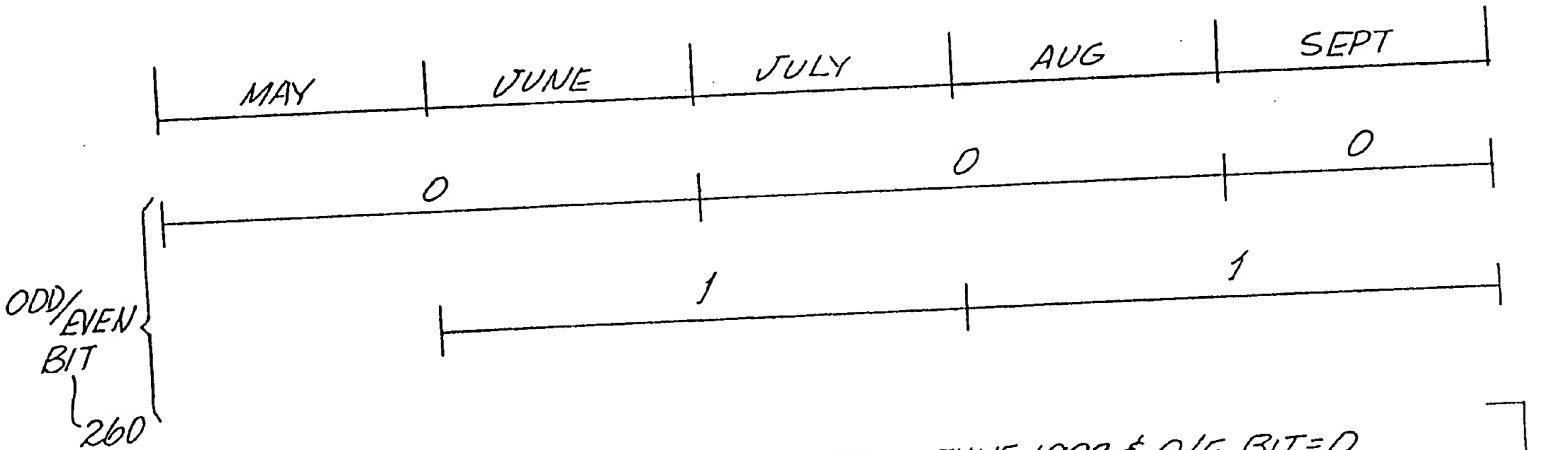


Fig. 6

DOCID: <WO___9517059A1_L>

Fig. 7



EXAMPLE: IF VCR CLOCK INDICATES JUNE 1993 & O/E BIT=0
THEN KEY GENERATED BASED ON DATE OF MAY 1993
IF VCR CLOCK INDICATES JUNE 1993 & O/E BIT=1
THEN KEY GENERATED BASED ON DATE OF JUNE 1993

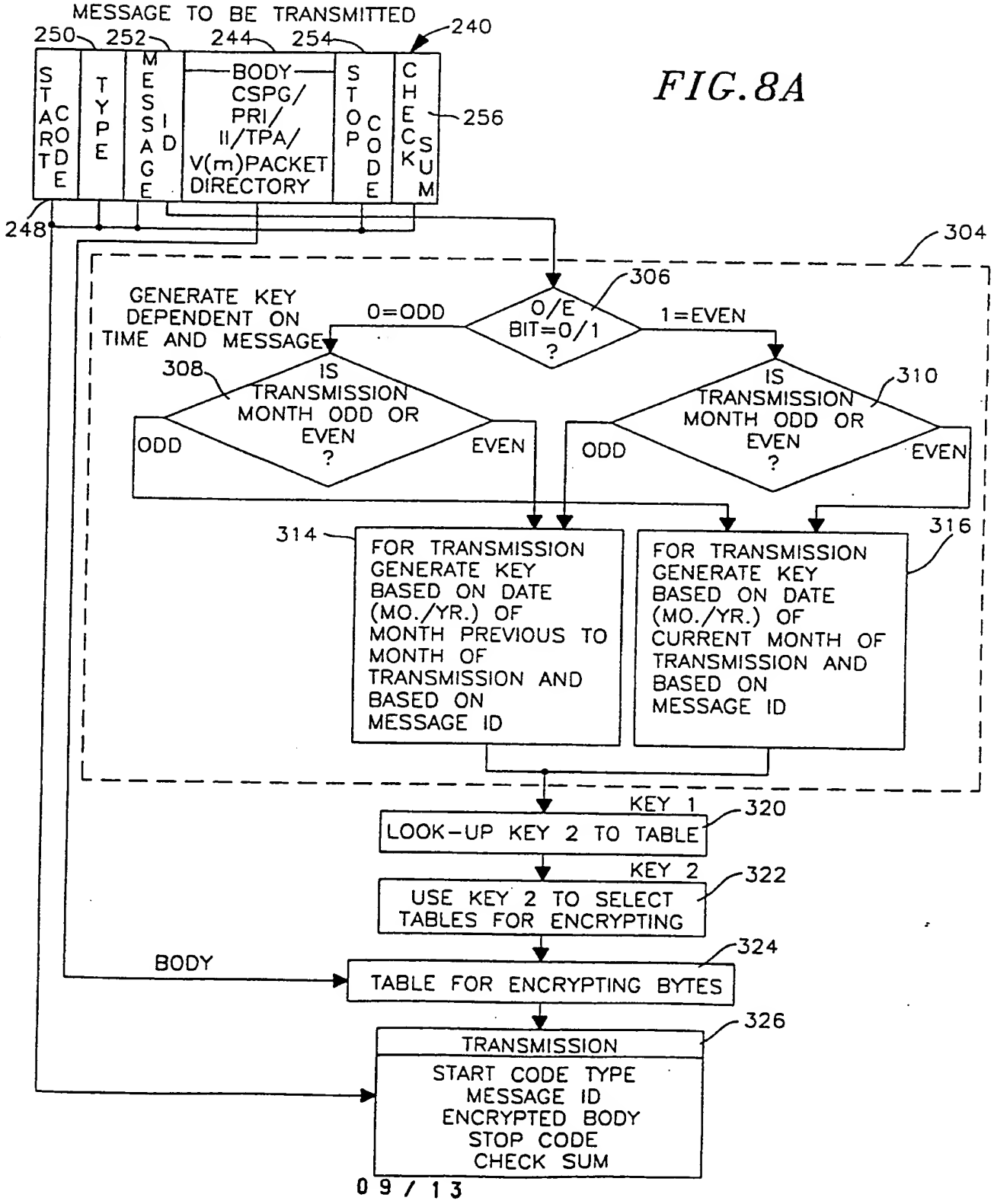
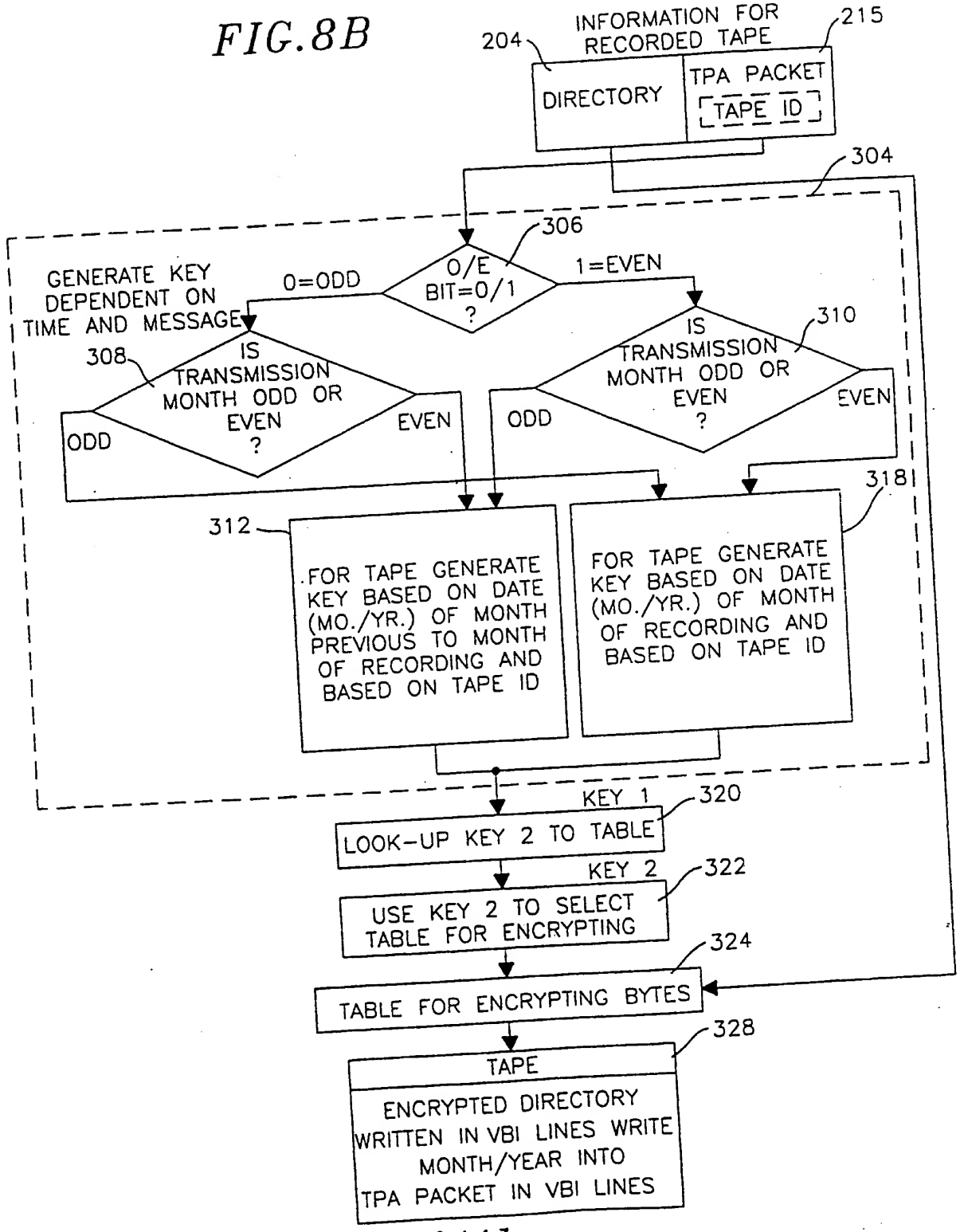


FIG. 8A

XOCID: <WO__9517059A1_I_>

FIG.8B


INFORMATION FOR RECORDED TAPE
215
204
DIRECTORY
TPA PACKET
TAPE ID
304
306
GENERATE KEY DEPENDENT ON TIME AND MESSAGE
0/E BIT=0/1 ?
0=ODD
1=EVEN
308
IS TRANSMISSION MONTH ODD OR EVEN ?
ODD
EVEN
310
IS TRANSMISSION MONTH ODD OR EVEN ?
ODD
EVEN
312
FOR TAPE GENERATE KEY BASED ON DATE (MO./YR.) OF MONTH PREVIOUS TO MONTH OF RECORDING AND BASED ON TAPE ID
318
FOR TAPE GENERATE KEY BASED ON DATE (MO./YR.) OF MONTH OF RECORDING AND BASED ON TAPE ID
KEY 1
320
LOOK-UP KEY 2 TO TABLE
KEY 2
322
USE KEY 2 TO SELECT TABLE FOR ENCRYPTING
324
TABLE FOR ENCRYPTING BYTES
328
TAPE
ENCRYPTED DIRECTORY WRITTEN IN VBI LINES WRITE MONTH/YEAR INTO TPA PACKET IN VBI LINES

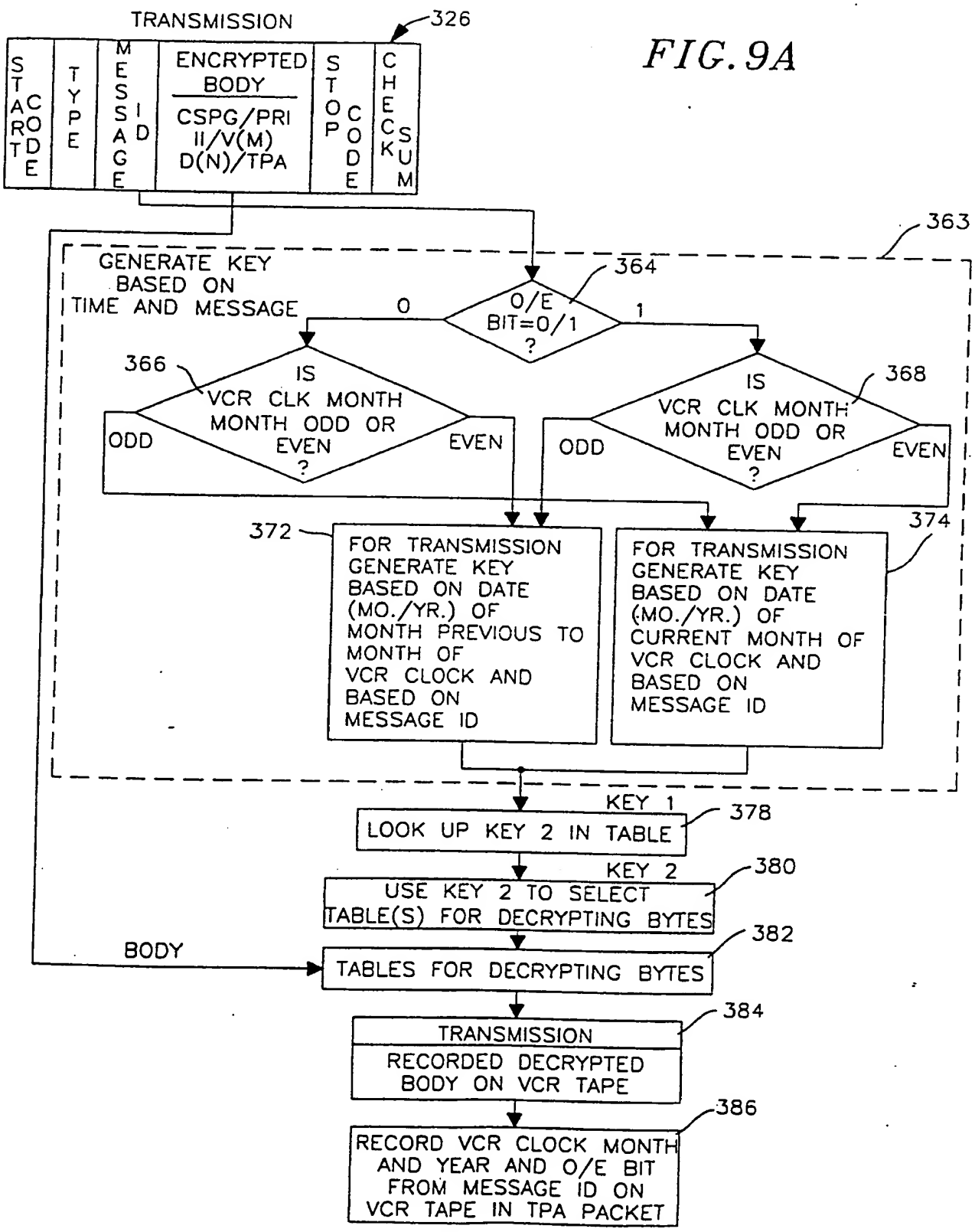
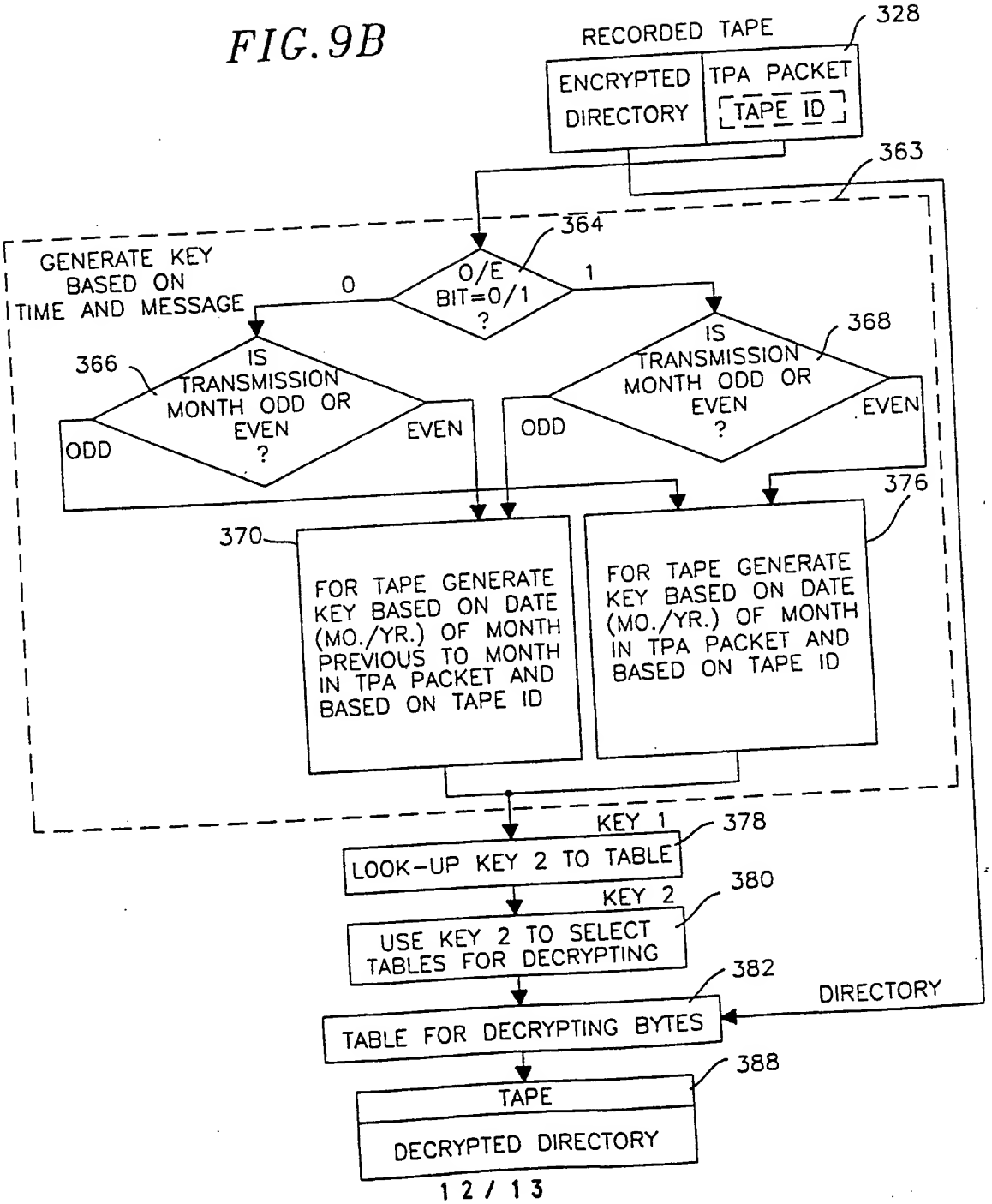


FIG. 9A

DOCID: <WO__9517059A1_I_>

FIG. 9B


RECORDED TAPE
328
ENCRYPTED DIRECTORY
TPA PACKET
TAPE ID
363
364
GENERATE KEY BASED ON TIME AND MESSAGE
O/E BIT=0/1 ?
0
1
366
IS TRANSMISSION MONTH ODD OR EVEN ?
ODD
EVEN
368
IS TRANSMISSION MONTH ODD OR EVEN ?
ODD
EVEN
370
FOR TAPE GENERATE KEY BASED ON DATE (MO./YR.) OF MONTH PREVIOUS TO MONTH IN TPA PACKET AND BASED ON TAPE ID
376
FOR TAPE GENERATE KEY BASED ON DATE (MO./YR.) OF MONTH IN TPA PACKET AND BASED ON TAPE ID
KEY 1
378
LOOK-UP KEY 2 TO TABLE
KEY 2
380
USE KEY 2 TO SELECT TABLES FOR DECRYPTING
382
TABLE FOR DECRYPTING BYTES
DIRECTORY
388
TAPE
DECRYPTED DIRECTORY

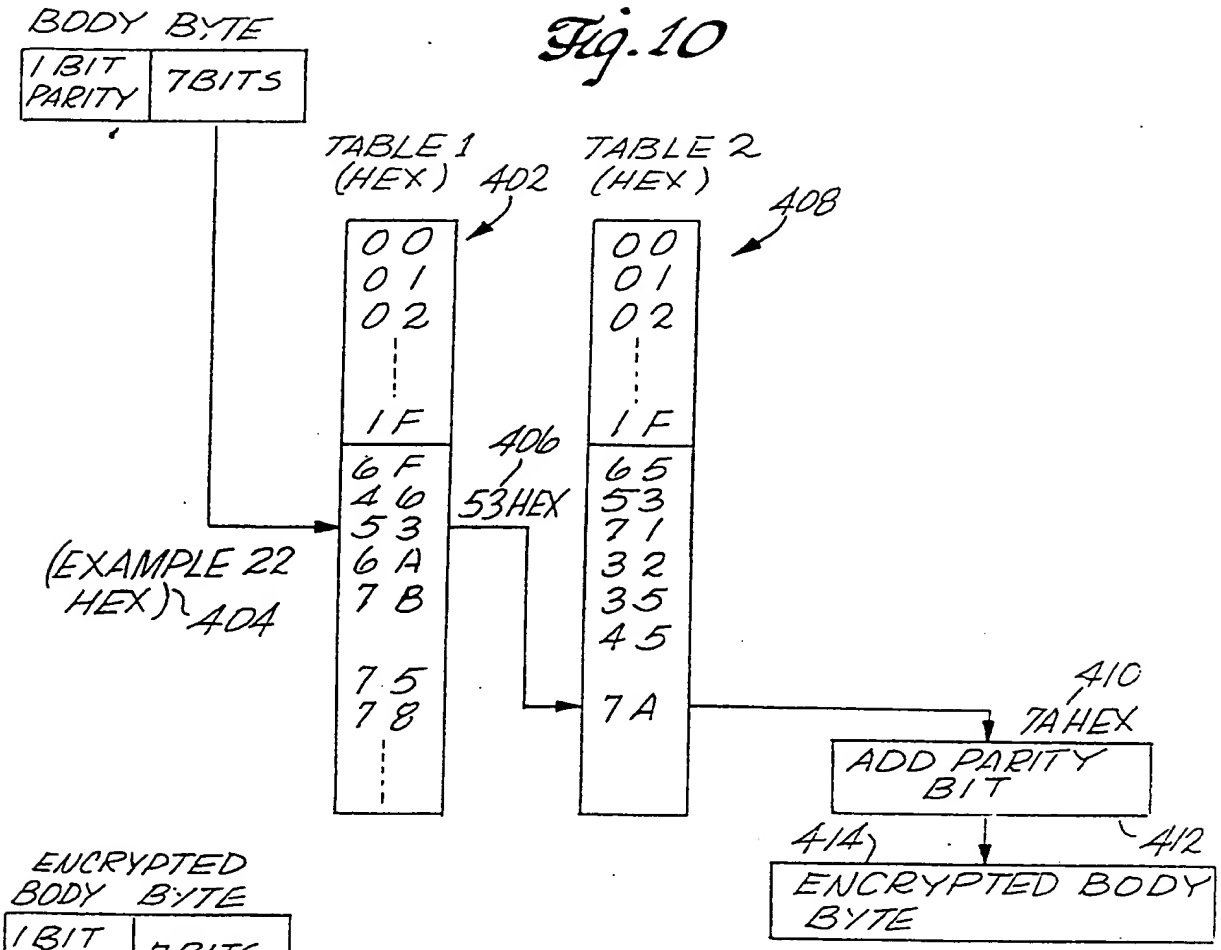


Fig. 10

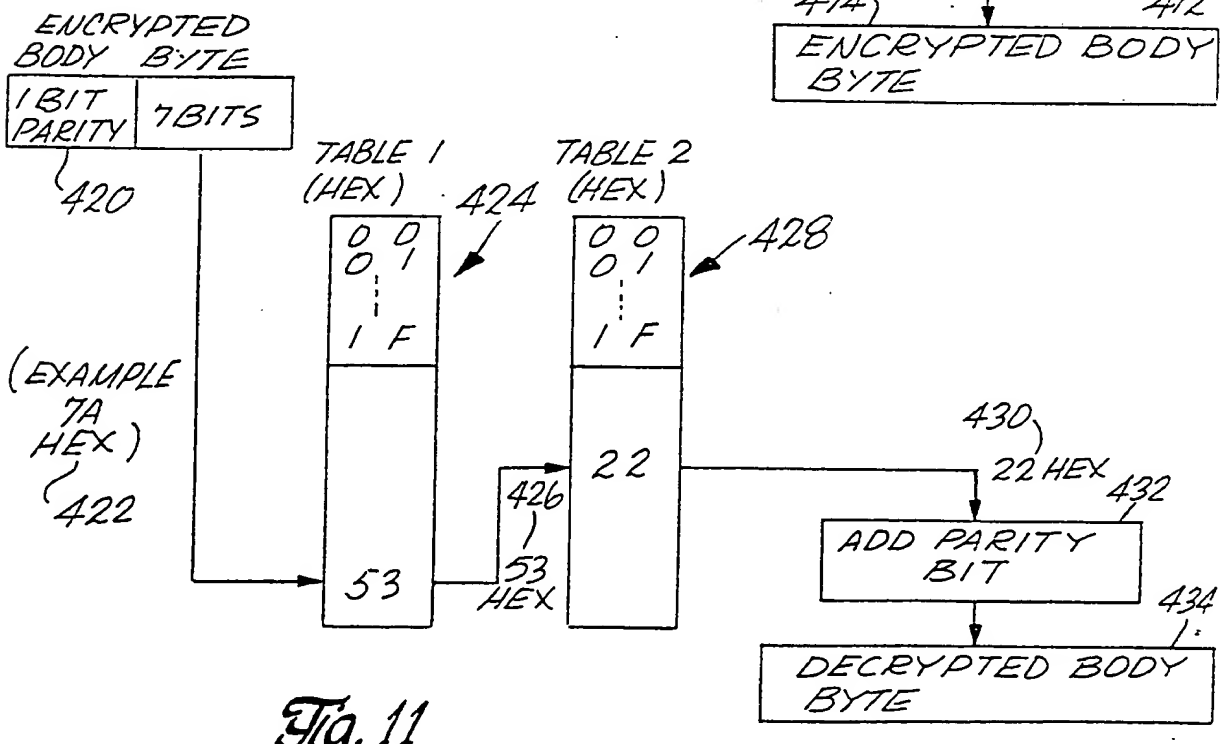


Fig. 11

DCID: <WO___9517069A1_L>

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US94/14309

A. CLASSIFICATION OF SUBJECT MATTER
IPC(6) :H04L 9/08
US CL :380/5, 10, 18, 20, 21
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED
Minimum documentation searched (classification system followed by classification symbols)
U.S. : 380/5, 10, 18, 20, 21

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US, A, 4,636,854 (CROWTHER ET AL.) 13 JANUARY 1987, SEE FIG. 2.	1-23
Y	US, A, 4,866,770 (SETH-SMITH ET AL.) 12 SEPTEMBER 1989, SEE FIGS. 10-12 COLS. 16-17.	1-23
Y	US, A, 4,829,569 (SETH-SMITH ET AL.) 09 MAY 1989, SEE FIGS. 10-14.	1-23
Y	US, A, 4,890,321 (SETH-SMITH ET AL) 26 DECEMBER 1989, SEE ENTIRE DOCUMENT.	1-23
Y	US, A, 5,081,678 (KAUFMAN ET AL.) 14 JANUARY 1992, SEE FIG. 3.	26-27
Y	US, A, 5,222,136 (RASMUSSEN ET AL.) 22 JUNE 1993, SEE FIGS. 5-6.	24-27

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be part of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search
07 APRIL 1995

Date of mailing of the international search report
04 MAY 1995

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703) 305-3230

Authorized officer
SALVATORE CANGIALOSI
Telephone No. (703) 308-0482

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US94/14309

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No
Y	US, A, 4,890,319 (SETH-SMITH ET AL.) 26 DECEMBER 1989, SEE FIGS. 10-15.	24-37
Y	US, A, 4,937,866 (CROWTHER ET AL.) 26 JUNE 1990, SEE FIG. 8.	24-37
Y	US, A, 5,146,495 (SON) 08 SEPTEMBER 1992, SEE FIGS. 4-5.	28-34
Y	US, A, 4,663,659 (BLATTER) 05 MAY 1987, SEE FIGS. 1-3, 6, 10- 11.	28-34
Y	US, B, 4,706,121 (YOUNG) 14 DECEMBER 1993, SEE FIGS. 4, 4B, 8, 10, 11 AND 13.	35-37
Y	US, A, 5,172,413 (BRADLEY ET AL.) 15 DECEMBER 1992, SEE FIG. 4.	35-37
Y	US, A, 4,706,121 (YOUNG) 10 NOVEMBER 1987, SEE FIGS. 4, 4B, 8, 10, 11 AND 13.	35-37

DCID: <WO___9517069A1_I_>

INTERNATIONAL SEARCH REPORT

International application No
PCT/US94/14309

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

Please See Extra Sheet.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☒ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No
PCT/US94/14309

BOX II. OBSERVATIONS WHERE UNITY OF INVENTION WAS LACKING
This ISA found multiple inventions as follows:

Group I, Claims 1-23, drawn to a method of embedding a time base key in a video program.

Group II, claims 24-27, drawn to a method of generating a scrambling key from header of a video program.

Group III, claims 28-34, drawn to a method and apparatus of including a tape identification number in a video tape.

Group IV, claims 35-37, drawn to a method of detecting user selections.

The inventions listed as groups I-IV do not relate to a single inventive concept under PCT Rule 13.1, because under PCT Rule 13.2, they lack the same or corresponding technical features for the following reasons:

The invention of Groups II-IV lack the technical feature of a time based scrambling key.

The inventions of Groups I, III & IV lack the technical feature of generating a scrambling key from header information.

The inventions of Groups I, II and IV lack the technical feature of including a tape identification number

The inventions of Groups I-III lack the technical feature of detecting user selections.

CID: <WO___9617069A1_I_>

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/08 A1

(11) International Publication Number: WO 95/17059

(43) International Publication Date: 22 June 1995 (22.06.95)

(21) International Application Number: PCT/US94/14309

(22) International Filing Date: 14 December 1994 (14.12.94)

(30) Priority Data:
08/167,678 15 December 1993 (15.12.93) US
08/183,602 18 January 1994 (18.01.94) US

(71)(72) Applicants and Inventors: MANKOVITZ, Roy, J. [US/US]; 18057 Medley Drive, Encino, CA 91316 (US). NG, Yee, Kong [GB/GB]; 18 H Block 4, Uptown Plaza, Tai Po, N.T. (HK).

(74) Agent: HARTZ, Edwin, L.; Christie, Parker & Hale, P.O. Box 7068, Pasadena, CA 91109-7068 (US).

(81) Designated States: AM, AT, AU, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, JP, KE, KG, KP, KR, KZ, LK, LR, LT, LU, LV, MD, MG, MN, MW, NL, NO, NZ, PL, PT, RO, RU, SD, SE, SI, SK, TJ, TT, UA, UZ, VN, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), ARIPO patent (KE, MW, SD, SZ).

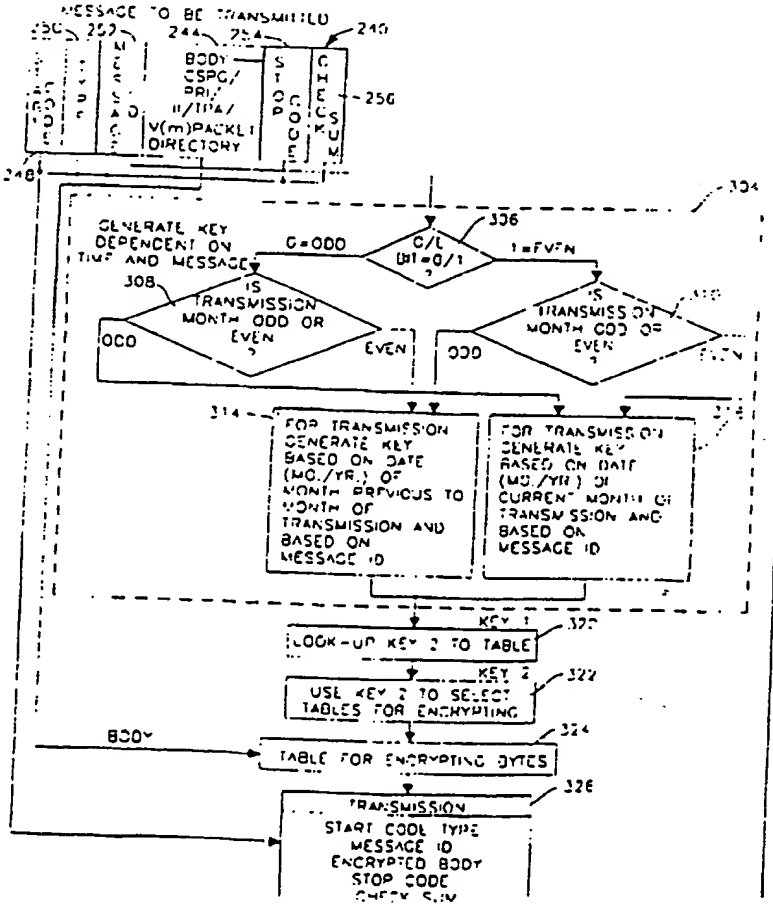
Published
With international search report.
With amended claims.

Date of publication of the amended claims:
13 July 1995 (13.07.95)

(54) Title: METHOD FOR ENCRYPTING AND EMBEDDING INFORMATION IN A VIDEO PROGRAM

(57) Abstract

A method is provided for transmitting information having a header portion (242) and a body portion (244), the method includes the steps of providing a clock (80), generating (316) a first key base on the clock (80) and a part of the header portion (242), using the first key for encrypting the body portion (244) to generate an encrypted body portion, combining the encrypted body portion and the header portion to form a data packet (240), combining a video program and the data packet (240) to form and transmit a composite video signal (326). After encryption the encrypted body portion can be scrambled by using a scrambling key to swap the bits of the body portion. A method for receiving transmitted information having a header portion (242) and an encrypted body portion comprises the steps of providing a clock (80), generating (318) a first key based on the clock (80) and a part of the header portion (242), using the first key for decrypting the encrypted body portion to generate a decrypted body portion, combining the decrypted body portion and the header portion to form a data packet, and recording the data packet on a video cassette tape (328).



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria
AU	Australia
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CS	Czechoslovakia
CZ	Czech Republic
DE	Germany
DK	Denmark
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgystan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakhstan
LI	Liechtenstein
LK	Sri Lanka
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SI	Slovenia
SK	Slovakia
SN	Senegal
TD	Chad
TG	Togo
TJ	Tajikistan
TT	Trinidad and Tobago
UA	Ukraine
US	United States of America
UZ	Uzbekistan
VN	Viet Nam

38. A method for encrypting information having a header portion and a body portion comprising the steps of:

obtaining a month from a clock having an output as a function of time;

setting an odd/even month indication in the header portion to odd, if the month obtained from the clock is an odd month;

setting an odd/even month indication in the header portion to even, if the month obtained from the clock is an even month;

generating a first key as a function of the month obtained from the clock and the odd/even month indication set in the header portion;

using the first key for encrypting the body portion to generate an encrypted body portion; and

embedding the encrypted body portion and the header portion within a video program to form a composite video signal.

39. The method of claim 38 further comprising the step of transmitting the composite video signal.

40. The method of claim 38 further comprising the step of recording the composite video signal.

41. The method of Claim 38 further comprising the steps of:

obtaining a scrambling key from the header portion; and

scrambling the encrypted body portion using the scrambling key.

42. The method of Claim 41 wherein the step of scrambling the encrypted body portion using the scrambling key comprises the steps of:

assigning each bit of the scrambling key to a number of pairs of characters in the encrypted body portion;

swapping the characters of the pair, if the assigned bit is of a first type;

otherwise, not swapping the characters of the pair, if the assigned bit is of a second type; and

repeating the steps of swapping or not swapping for all pairs of characters of the encrypted body portion.

43. The method of Claim 38 wherein the step of embedding the encrypted body portion and the header portion within a video program to form a composite video signal comprises the step of embedding the encrypted body portion and the header portion into vertical blanking interval lines of the video program.

DOCID: <WO__9517060A1_IA>

44. The method of Claim 38 wherein the step of using the first key for encrypting the body portion to generate an encrypted body portion comprises the steps of:

using the first key to select a first table;

mapping each part of the body portion to a first encrypted part using the first table; and

concatenating each first encrypted part to form an encrypted body portion.

45. The method of Claim 44 wherein the step of mapping each part of the body portion to a first encrypted part using the first table comprises the steps of:

using the first key to select a second table; and

mapping each first encrypted part to a second encrypted part using the second table.

46. The method of Claim 38 wherein the step of generating a first key as a function of the month obtained from the clock and the odd/even month indication set in the header portion comprises the step of performing a table lookup.

47. A method for decrypting information in a composite video signal having an embedded header portion and an encrypted body portion, the method comprising the steps of:

reading a month from a clock having an output as a function of time;

extracting an odd/even month indication from the header portion;

generating a first key based on a month previous to the month read from the clock, if the odd/even month indication is odd and the month read from the clock is an even month or if the odd/even month indication is even and the month read from the clock is an odd month;

generating the first key based on the month read from the clock, if the odd/even month indication is odd and the month read from the clock is an odd month or if the odd/even month indication is even and the month read from the clock is an even month; and

using the first key for decrypting the encrypted body portion to generate a decrypted body portion.

48. The method of claim 47 further comprising the steps of:

combining the decrypted body portion and the header portion to form a data packet; and

recording the data packet on a video cassette tape.

49. The method of Claim 47 further comprising the steps of:

obtaining a scrambling key from the header portion; and

descrambling the encrypted body portion using the scrambling key.

50. The method of Claim 49 wherein the step of descrambling the encrypted body portion using the scrambling key comprises the steps of:

assigning each bit of the scrambling key to a number of pairs of characters in the encrypted body portion;

swapping the characters of the pair, if the assigned bit is of a first type;

otherwise, not swapping the characters of the pair, if the assigned bit is of a second type; and

repeating the steps of swapping or not swapping for all pairs of characters of the encrypted body portion.

51. The method of Claim 47 further comprising the step of decoding a vertical blanking interval to extract the embedded headed portion and the encrypted body portion from the composite video signal.

52. The method of Claim 47 wherein the step of using the first key for decrypting the encrypted body portion to generate a decrypted body portion comprises the steps of:

using the first key to select a first table;

mapping each part of the encrypted body portion to a first decrypted part using the first table; and

concatenating each first decrypted part to form an decrypted body portion.

53. The method of Claim 52 wherein the step of mapping each part of the encrypted body portion to a first decrypted part using the first table comprises the steps of:

using the first key to select a second table; and

mapping each first decrypted part to a second decrypted part using the second table.

54. The method of Claim 47 wherein the step of generating a first key as a function of the month read from the clock comprises the step of performing a table lookup.

55. The method of Claim 47 further comprising the step of receiving a transmitted composite video signal having an embedded header portion and an encrypted body portion.

56. The method of Claim 47 further comprising the step of receiving a recorded composite video signal having an embedded header portion and an encrypted body portion.

XOCID: <WO___9517069A1_IA>

THIS PAGE BLANK (USPTO)